

OSM Service Connection User's Guide

HP Part Number: 527274-045

Published: August 2014

Edition: J06.03 and subsequent J-series RVUs and H06.03 and subsequent H-series RVUs.



Legal Notice

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Export of the information contained in this publication may require authorization from the U.S. Department of Commerce.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Intel, Pentium, and Celeron are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Motif, OSF/1, UNIX, X/Open, and the "X" device are registered trademarks, and IT DialTone and The Open Group are trademarks of The Open Group in the U.S. and other countries.

Open Software Foundation, OSF, the OSF logo, OSF/1, OSF/Motif, and Motif are trademarks of the Open Software Foundation, Inc. OSF MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE OSF MATERIAL PROVIDED HEREIN, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. OSF shall not be liable for errors contained herein or for incidental consequential damages in connection with the furnishing, performance, or use of this material.

© 1990, 1991, 1992, 1993 Open Software Foundation, Inc. The OSF documentation and the OSF software to which it relates are derived in part from materials supplied by the following: © 1987, 1988, 1989 Carnegie-Mellon University. © 1989, 1990, 1991 Digital Equipment Corporation. © 1985, 1988, 1989, 1990 Encore Computer Corporation. © 1988 Free Software Foundation, Inc. © 1987, 1988, 1989, 1990, 1991 Hewlett-Packard Company. © 1985, 1987, 1988, 1989, 1990, 1991, 1992 International Business Machines Corporation. © 1988, 1989 Massachusetts Institute of Technology. © 1988, 1989, 1990 Mentat Inc. © 1988 Microsoft Corporation. © 1987, 1988, 1989, 1990, 1991, 1992 SecureWare, Inc. © 1990, 1991 Siemens Nixdorf Informationssysteme AG. © 1986, 1989, 1996, 1997 Sun Microsystems, Inc. © 1989, 1990, 1991 Transarc Corporation. OSF software and documentation are based in part on the Fourth Berkeley Software Distribution under license from The Regents of the University of California. OSF acknowledges the following individuals and institutions for their role in its development: Kenneth C.R.C. Arnold, Gregory S. Couch, Conrad C. Huang, Ed James, Symmetric Computer Systems, Robert Elz. © 1980, 1981, 1982, 1983, 1985, 1986, 1987, 1988, 1989 Regents of the University of California.

Contents

What's New in This Guide.....	32
About This Guide.....	40
Related Reading.....	41
1 Introducing OSM.....	42
OSM Interfaces.....	42
OSM Service Connection.....	42
OSM Guided Procedures.....	42
OSM Low-Level Link.....	43
OSM Event Viewer.....	43
2 Preparing the OSM Environment.....	44
Installing OSM Components.....	44
System Console-Based Components.....	44
Server-Based Components.....	44
Using OSM in Conjunction with HP SIM.....	44
3 Configuring OSM.....	45
Enabling Java Next Generation Plug-in to Avoid OSM Memory Errors.....	45
Configuring the Server.....	46
Defining Users.....	46
MSP (Low-Level-Link) Users.....	46
NonStop Operating System Users.....	46
How to Plan Your Users.....	46
Configuring OSM Power-Fail Support.....	46
4 Starting the OSM Service Connection.....	48
Launching an OSM Service Connection.....	48
OSM Service Connection Session Error Messages.....	49
Using OSM Bookmarks.....	49
Verifying the OSM Service Connection State.....	49
Running Multiple Sessions.....	49
5 Using the Management Window.....	51
Management Window Example.....	52
Internet Explorer Menu Bar.....	52
OSM Menu Bar Options.....	52
Display Menu.....	53
Summary Menu.....	53
Tools Menu.....	53
Windows Menu.....	54
Help Menu.....	54
Rediscover Shortcut Menu Item.....	54
Using the Physical View.....	55
Physical View of the ServerNet Cluster.....	55
Physical View of a Local System.....	55
Physical View of an Enclosure.....	55
Physical View of a Fabric.....	56
Using the Inventory View.....	56
Inventory View of a ServerNet Cluster.....	56
Inventory View of a Local System.....	57
Using Shortcut Menus.....	57
Interpreting Icons and Color.....	58

State Indicators.....	58
Alarm Indicators.....	59
In the tree pane.....	59
On the alarms tab and detail.....	59
In the Alarm Summary.....	59
Alarm Severity.....	59
Using the Browser's Find Feature.....	60
6 Viewing Alarms.....	61
Viewing the Alarms Tab.....	61
Viewing the Alarms Dialog Box.....	62
Viewing Alarm Details.....	62
Suppressing Alarms.....	63
Deleting Alarms.....	63
7 Viewing Attributes.....	64
Using the Details Pane to View Attributes.....	64
Using the Attributes Dialog Box to View Attributes.....	64
Suppressing Problem Attributes.....	64
8 Performing Actions.....	66
Controlling Access to Actions.....	66
Migrating Access Control List Settings.....	68
Performing Actions on a Selected Resource.....	68
Performing an Action.....	68
Viewing Detailed Information About an Action.....	69
Aborting an Action.....	69
Performing Actions on Multiple Resources of the Same Type.....	69
Performing an Action.....	69
Saving a Multi-Resource View.....	70
Using Customized Resource Views.....	70
Creating and Saving a Customized Resource View.....	70
Selecting a Saved Resource View.....	70
Deleting a Resource View.....	70
Viewing Action Details.....	71
Performing Firmware Updates.....	71
Performing a Firmware Update.....	71
Launching Guided Procedures.....	72
Using the Physical Configuration Tool.....	72
9 Viewing Summary Reports.....	74
Viewing a Problem Summary.....	74
Viewing a Summary of Actions.....	74
Actions Not Displayed.....	74
OSM Software-Triggered Actions.....	74
Viewing Action Details.....	74
Viewing a Summary of Alarms.....	74
Viewing a Resource Summary.....	75
10 Managing a System.....	76
Locating and Viewing System Resources.....	76
Monitoring a System.....	76
Performing Actions on a System.....	76
Updating Firmware.....	76
11 System Resources.....	77
4PSE (4-Port ServerNet Extender).....	78
Attributes.....	78

Physical.....	78
Logical.....	78
Actions.....	78
Power Off.....	78
Power On.....	78
Replace.....	78
Set LED State.....	79
Alarm Panel (Telco).....	79
Attributes.....	79
Alarm Panel.....	79
Physical.....	79
Physical Location.....	79
Actions.....	80
Link to Web Interface.....	80
Rediscover.....	80
Stop Monitoring.....	80
ATM3SA (ATM Adapter).....	80
Attributes.....	80
ATM3SA.....	80
Physical.....	80
Logical.....	80
Firmware.....	81
Actions.....	81
Abort.....	81
Firmware Update.....	81
Responsive Test.....	81
Start.....	81
Test Verify.....	82
ATM Line.....	82
Attributes.....	82
Line \$ATM.....	82
Logical.....	82
Actions.....	82
Battery.....	83
Attributes.....	83
Battery.....	83
Physical.....	83
Logical.....	83
Upper Voltage Sensor.....	83
Lower Voltage Sensor.....	83
Differential Voltage Sensor.....	83
Total Voltage Sensor.....	84
Actions.....	84
Enable/Disable.....	84
Blade Complex.....	84
Attributes.....	84
Blade Complex.....	84
Logical.....	84
Actions.....	85
Clear Activity in Progress.....	85
Firmware Update.....	85
Perform Cable Check.....	85
Set Activity in Progress.....	85
Set Processor Expected Redundancy.....	85
Blade Element.....	85

Attributes.....	86
Blade Element.....	86
Physical.....	86
Physical Location.....	87
Actions.....	87
Check If Safe to Replace.....	87
Check Reintegration Status.....	87
Clear Forward Progress Log.....	87
Disable Blade Element Reintegration.....	87
Enable Blade Element Reintegration.....	88
Firmware Update.....	88
Power Down Blade Element.....	88
Propagate System Name.....	88
Replace.....	88
Reset Blade Element.....	88
Retrieve and Clear BMC Event Log.....	88
Retrieve and Clear BMC Event Log - Formatted.....	88
Retrieve Forward Progress Log.....	89
Save Extended Inventory.....	89
Set LED State.....	89
Set Locator LED State.....	89
Set Optics Adapter LED State.....	89
Set Physical Location.....	89
Switch to Use Shadow Firmware Image After Reset.....	89
Switch to Use Running Firmware Image After Reset.....	90
Blade Element Firmware.....	90
Attributes.....	90
Blade Element Firmware.....	90
Halted State Services Firmware.....	90
Primitive State Firmware.....	91
Disk Boot Firmware.....	91
ISP1040 Firmware.....	91
Baseboard Management Controller Firmware.....	91
PAL/SAL Firmware.....	92
Actions.....	92
Blade System Board.....	92
Attributes.....	92
Blade System Board.....	92
Physical.....	92
Actions.....	92
Blower (FCDM).....	92
Attributes.....	93
Blower.....	93
Physical.....	93
Logical.....	93
Actions.....	93
Blink LED Off.....	93
Blink LED On.....	93
Replace.....	93
CCSA (Common Communication ServerNet Adapter).....	93
Attributes.....	93
CCSA.....	93
Physical.....	94
Logical.....	94
Actions.....	94

Abort.....	94
Start.....	94
Stop.....	94
Test Verify.....	94
CLIM.....	94
Attributes.....	95
CLIM.....	95
Logical.....	95
Physical.....	97
Physical Location.....	97
X1 Fabric Information.....	97
X2 Fabric Information.....	97
Y1 Fabric Information.....	97
Y2 Fabric Information.....	97
iLO.....	97
ROM.....	98
Actions.....	98
Backup CLIM Configuration.....	98
Collect CLIM Logs	98
Delete.....	98
iLO Update.....	98
Invoke iLO.....	98
Reboot.....	98
Replace.....	98
Replace Hard Drive.....	99
Restore CLIM Configuration.....	99
Restore Default Storage Path Configuration.....	99
ROM Update.....	99
Set UID LED State.....	99
Show CLIM/Key Manager Registration Information.....	99
Start.....	99
Stop.....	99
Stop Storage Paths.....	99
Switch Storage Paths Away.....	99
CLIMs.....	99
Attributes.....	100
Actions.....	100
Collect CLIM Logs	100
Configure CLIM.....	100
Prepare for Down System CLIM Firmware Update.....	100
Register CLIMs with Key Managers.....	102
Set Location for CLIM Log Collection.....	102
CLIM-Attached Disks.....	102
Attributes.....	102
Actions.....	102
DIMM (CLIM).....	103
Attributes.....	103
DIMM.....	103
Logical.....	103
Actions.....	103
Replace.....	103
Disk.....	103
Attributes.....	103
Disk.....	103
Physical.....	104

Logical.....	104
Process Pair.....	104
Disk Pair.....	104
Firmware.....	104
Backup Path.....	105
Primary Path.....	105
Actions.....	105
Abort Backup Path.....	105
Abort Disk.....	105
Abort Primary Path.....	105
Clear Data.....	105
Firmware Update.....	105
Power Off.....	106
Power On.....	106
Reset Backup Path.....	106
Reset Disk.....	106
Reset Primary Path.....	106
Reset Volume.....	106
Responsive Test.....	106
Save as System Load Configuration.....	106
Start Backup Path.....	107
Start Disk.....	107
Start Primary Path.....	107
Start Volume.....	107
Stop Backup Path.....	107
Stop Disk.....	107
Stop Primary Path.....	107
Stop Volume.....	107
Switch Process Pair.....	108
Switch to Backup Path.....	108
Switch to Primary Path.....	108
Test Verify.....	108
Validate Checksum.....	108
Disk (CLIM-Attached).....	108
Attributes.....	108
Disk.....	108
Logical.....	108
Backup Path.....	109
Disk Pair.....	109
Primary Path.....	109
Process Pair.....	109
Actions.....	109
Abort Backup Path.....	109
Abort Disk.....	110
Abort Primary Path.....	110
Clear Data.....	110
Reset Backup Path.....	110
Reset Disk.....	110
Reset Primary Path.....	110
Reset Volume.....	110
Responsive Test.....	110
Save as System Load Configuration.....	110
Set LED State.....	110
Start Backup Path.....	111
Start Disk.....	111

Start Primary Path.....	111
Start Volume.....	111
Stop Backup Path.....	111
Stop Disk.....	111
Stop Primary Path.....	111
Stop Volume.....	111
Switch Process Pair.....	111
Switch to Backup Path.....	111
Switch to Primary Path.....	111
Disk (Fibre Channel).....	111
Attributes.....	112
Disk (Fibre Channel).....	112
Physical.....	112
Logical.....	112
Process Pair.....	112
Disk Pair.....	113
Primary Path.....	113
Backup Path.....	113
Firmware.....	113
Actions.....	113
Abort Backup Path.....	113
Abort Disk.....	113
Abort Primary Path.....	114
Blink LED Off.....	114
Blink LED On.....	114
Clear Data.....	114
Disable Drive Bypass.....	114
Enable Drive Bypass.....	114
Firmware Update.....	114
Replace.....	114
Reset Backup Path.....	114
Reset Disk.....	114
Reset Primary Path.....	114
Reset Volume.....	114
Responsive Test.....	115
Save as System Load Configuration.....	115
Spin Down.....	115
Spin Up.....	115
Start Backup Path.....	115
Start Disk.....	115
Start Primary Path.....	115
Start Volume.....	115
Stop Backup Path.....	116
Stop Disk.....	116
Stop Primary Path.....	116
Stop Volume.....	116
Switch Process Pair.....	116
Switch to Backup Path.....	116
Switch to Primary Path.....	116
Verify Physical Connectivity.....	116
Disk (SAS).....	116
Attributes.....	116
Physical.....	116
Firmware.....	116
Actions.....	117

Firmware Update.....	117
Get Logical Disk(s).....	117
Replace.....	117
Set LED State.....	117
Show SMARTSSD Wear Gauge.....	117
Start Disk.....	117
Start Volume.....	117
Stop Disk.....	117
DVD-ROM (Blade Element).....	117
Attributes.....	117
DVD-ROM.....	117
Physical.....	117
Actions.....	117
E4SA (Ethernet 4 ServerNet Adapter).....	118
Attributes.....	118
E4SA.....	118
Physical.....	118
Logical.....	118
Actions.....	118
Abort.....	118
Disable ServerNet Port.....	118
Enable ServerNet Port.....	119
Start.....	119
Stop.....	119
EMU.....	119
Attributes.....	119
EMU.....	119
Physical.....	119
Logical.....	119
Firmware.....	119
Actions.....	119
Firmware Update.....	119
Replace.....	119
Enclosure.....	120
Attributes.....	120
Enclosure.....	120
Physical.....	120
Physical Location.....	120
Logical.....	120
Configuration.....	121
Actions.....	121
Configure a Power Source as AC.....	121
Configure a Power Source as UPS.....	121
Delete the Power Source Configuration.....	122
Display Diagnostic Status Errors.....	122
Launch the Onboard Administrator.....	122
Prepare Enclosure for Removal.....	122
Set Physical Location.....	122
ESS Disk.....	122
Attributes.....	122
ESS Disk.....	122
Logical.....	123
Backup Path.....	123
Primary Path.....	123
Disk Pair.....	123

Process Pair.....	123
Actions.....	124
Abort Backup Path.....	124
Abort Disk.....	124
Abort Primary Path.....	124
Reset Backup Path.....	124
Reset Disk.....	124
Reset Primary Path.....	124
Reset Volume.....	124
Responsive Test.....	124
Start Backup Path.....	124
Start Disk.....	124
Start Primary Path.....	124
Start Volume.....	125
Stop Backup Path.....	125
Stop Disk.....	125
Stop Primary Path.....	125
Stop Volume.....	125
Switch Process Pair.....	125
Switch to Backup Path.....	125
Switch to Primary Path.....	125
ESS Disk Collection.....	125
Attributes.....	125
External Disk.....	125
Attributes.....	126
External Disk.....	126
Physical.....	126
Logical.....	126
Process Pair.....	126
Disk Pair.....	126
Backup Path.....	127
Primary Path.....	127
Firmware.....	127
Actions.....	127
Abort Backup Path.....	127
Abort Disk.....	127
Abort Primary Path.....	127
BLINK LED Off.....	127
BLINK LED On.....	127
Clear Data.....	127
Firmware Update.....	128
Reset Backup Path.....	128
Reset Disk.....	128
Reset Primary Path.....	128
Reset Volume.....	128
Responsive Test.....	128
Start Backup Path.....	128
Start Disk.....	128
Start Primary Path.....	128
Start Volume.....	128
Stop Backup Path.....	128
Stop Disk.....	128
Stop Primary Path.....	129
Stop Volume.....	129
Switch to Backup Path.....	129

Switch to Primary Path.....	129
Test Verify.....	129
Validate Checksum.....	129
External Disk Collection.....	129
Attributes.....	129
Actions.....	129
Fan.....	129
Attributes.....	130
Fan.....	130
Physical.....	130
Logical.....	130
Rotations Sensor.....	130
Actions.....	130
Enable/Disable.....	130
Fan Assembly (Blade Element).....	130
Attributes.....	130
Fan Assembly	130
Physical.....	131
Logical.....	131
Actions.....	131
Fan (CLIM).....	131
Attributes.....	131
Fan	131
Logical.....	131
Actions.....	131
Replace.....	131
Fan (IOAM).....	131
Attributes.....	132
Physical.....	132
Logical.....	132
Actions.....	132
Set LED State.....	132
Fan (Processor Switch).....	132
Attributes.....	132
Physical.....	132
Logical.....	132
Actions.....	132
Replace.....	132
Set LED State.....	132
Fan (SAS Disk Enclosure).....	132
Attributes.....	133
Actions.....	133
Replace.....	133
Fan (VIO).....	133
Attributes.....	133
Physical.....	133
Logical.....	133
Actions.....	133
Replace.....	133
Set LED State.....	133
FC Card (CLIM).....	133
Attributes.....	133
Physical.....	133
Logical.....	134
BIOS.....	134

Firmware.....	134
Actions.....	134
BIOS Update.....	134
Firmware Update.....	134
Replace.....	134
FC-AL I/O Module.....	134
Attributes.....	134
FC-AL I/O Module.....	134
Physical.....	135
Logical.....	135
Device Connection.....	135
Actions.....	135
Blink LED Off.....	135
Blink LED On.....	135
Replace.....	135
FCDM.....	135
Attributes.....	136
FCDM.....	136
Physical.....	136
Physical Location.....	136
Logical.....	136
Path B.....	136
Path A.....	137
Actions.....	137
Blink All LEDs Off.....	137
Blink All LEDs On.....	137
Disable All Drive Bypass.....	137
Enable All Drive Bypass.....	137
Replace.....	137
Set Physical Location.....	137
Verify Path A Access.....	137
Verify Path B Access.....	138
FCDM Collection.....	138
Attributes.....	138
FCDM Collection.....	138
Path B.....	138
Path A.....	138
Actions.....	138
FCSA.....	138
Attributes.....	139
FCSA.....	139
Physical.....	139
Flash Firmware.....	139
Flash Boot Firmware.....	139
Actions.....	139
Flash Boot Firmware Update.....	139
Flash Firmware Update.....	139
Replace.....	140
Responsive Test.....	140
Test Verify.....	140
Removing and Installing a Fibre Channel ServerNet Adapter.....	140
Removing the FCSA.....	140
Installing the Replacement FCSA.....	141
FCSA FSAC.....	142
Attributes.....	142

FCSA FSAC.....	142
Actions.....	143
Responsive Test.....	143
FESA (Fast Ethernet ServerNet Adapter).....	143
Attributes.....	143
FESA.....	143
Physical.....	143
Logical.....	143
Actions.....	143
Abort.....	143
Start.....	144
Stop.....	144
Fiber.....	144
Attributes.....	144
Fiber.....	144
Logical.....	144
Actions.....	144
Fibre Channel Router.....	144
Attributes.....	144
Physical.....	144
Associated Device.....	145
Physical Location.....	145
Actions.....	145
Link to Web Interface.....	145
Rediscover.....	145
Stop Monitoring.....	145
FSAC (Fiber ServerNet Addressable Controller).....	145
Attributes.....	146
FSAC.....	146
Physical.....	146
Logical.....	146
Actions.....	146
Responsive Test.....	146
G4SA.....	146
Attributes.....	146
G4SA.....	146
Physical.....	147
Logical.....	147
Actions.....	147
Abort.....	147
Add.....	147
Delete.....	147
Power Off.....	147
Reset.....	147
Start.....	147
Stop.....	147
G4SA PIF.....	147
Attributes.....	148
G4SA PIF.....	148
Logical.....	148
Actions.....	148
Abort.....	148
Alter Interface Type.....	148
Configure LIF.....	148
Start.....	149

Stop.....	149
G4SA SAC.....	149
Attributes.....	149
G4SA SAC.....	149
Logical.....	149
Firmware.....	150
Actions.....	150
Abort.....	150
Dump.....	150
Firmware Update.....	150
Responsive Test.....	150
Start.....	150
Stop.....	150
Test Verify.....	150
GESA (Gigabyte Ethernet ServerNet Adapter).....	150
Attributes.....	151
GESA.....	151
Physical.....	151
Logical.....	151
Actions.....	151
Abort.....	151
Start.....	151
Stop.....	151
Group (IOMF2 or VIO).....	152
Attributes.....	152
Group.....	152
Logical.....	152
Actions.....	152
Power Off.....	152
Set Service LED State.....	152
Group (IOAM, Fabric, G16SE).....	153
Attributes.....	153
Group.....	153
Actions.....	153
Rediscover.....	153
Hard Disk (CLIM).....	154
Attributes.....	154
Hard Disk.....	154
Firmware.....	154
Physical.....	154
Logical.....	154
Actions.....	154
Replace.....	154
InfiniBand HCA Card (CLIM).....	154
Attributes.....	154
Infiniband HCA Card.....	209
Logical.....	209
Physical.....	209
Firmware.....	209
Actions.....	155
Firmware Update.....	155
Replace.....	155
Internal ServerNet Fabric.....	155
Attributes.....	156
Actions.....	156

Group Connectivity ServerNet Path Test.....	156
Processor-to-Processor Connectivity Test.....	156
Start ServerNet.....	156
Stop ServerNet.....	156
IO Module.....	156
Attributes.....	156
Actions.....	156
Replace.....	156
IOAM (I/O Adapter Module).....	156
Attributes.....	157
Physical.....	157
Actions.....	157
Read LCD.....	157
Retrieve Network Connectivity Info.....	157
Synchronize FIR Files to Other Switches.....	157
Write LCD Line.....	157
IOAM Enclosure.....	157
Attributes.....	158
IOAM Enclosure.....	158
Physical Location.....	158
Actions.....	158
Replace IOAM Enclosure or ServerNet Switch Board.....	158
Set Physical Location.....	158
IOMF2 (I/O Multifunction 2).....	159
Attributes.....	159
IOMF2.....	159
Physical.....	159
Logical.....	159
Storage ASIC.....	160
Actions.....	160
Disable ServerNet Port.....	160
Enable ServerNet Port.....	160
Force Power Off.....	160
Power Off.....	160
Prepare to Power Off.....	160
Replace.....	161
Storage ASIC Initialization Test.....	161
Test Verify.....	161
LIF.....	161
Attributes.....	161
LIF.....	161
Logical.....	161
Actions.....	161
Abort.....	161
Delete.....	161
Start.....	161
Stop.....	161
Logical Processor.....	162
Attributes.....	162
Logical Processor.....	162
Logical.....	162
Physical.....	163
X Fabric Connection.....	163
Y Fabric Connection.....	163
Actions.....	163

Disable Processor Freeze.....	163
Enable Processor Freeze.....	164
Halt.....	164
Power Cycle LSU.....	164
Reclaim Memory Pages.....	164
Reload.....	164
Responsive Test.....	164
Soft Reset.....	164
Maintenance PIC.....	165
Attributes.....	165
Physical.....	165
Actions.....	165
Replace.....	165
Set LED State.....	165
Maintenance Switch.....	165
Attributes.....	165
Maintenance Switch.....	165
Physical.....	165
Physical Location.....	166
Actions.....	166
Link to Web Interface.....	166
Rediscover.....	166
Stop Monitoring.....	166
Memory Card (Blade Element).....	166
Attributes.....	167
Memory Card.....	167
Physical.....	167
Actions.....	167
Replace.....	167
Module.....	167
Attributes.....	167
Module.....	167
Physical Location.....	167
Temperature Sensor.....	168
Actions.....	168
Rediscover.....	168
Redundant Power Scrub.....	168
Set Physical Location.....	168
Monitored Service LAN Devices.....	169
Attributes.....	169
Actions.....	169
Start Monitoring Alarm Panel.....	169
Start Monitoring Fibre Channel Router.....	169
Start Monitoring Maintenance Switch.....	169
Start Monitoring UPS.....	169
Motherboard (CLIM).....	169
Attributes.....	170
Actions.....	170
Replace.....	170
NIC (CLIM).....	170
Attributes.....	170
NIC.....	170
Logical.....	170
Physical.....	170
Firmware.....	170

Actions.....	170
Firmware Update.....	170
Replace.....	171
Optical Extender PIC.....	171
Attributes.....	171
Physical.....	171
Logical.....	171
Actions.....	172
Power Off.....	172
Power On.....	172
Replace.....	172
Set LED State.....	172
PCI Riser.....	172
Attributes.....	172
PCI Riser.....	172
Actions.....	172
Replace.....	172
PIC.....	172
Attributes.....	172
PIC.....	172
Physical.....	172
Logical.....	173
Actions.....	173
Clear Loopback Test.....	173
Enable/Disable Port.....	173
External Loopback Test.....	173
When to Use the External Loopback Test.....	173
Internal Loopback Test.....	173
PIF.....	174
Attributes.....	174
PIF.....	174
Logical.....	174
Actions.....	175
Abort.....	175
Configure LIF.....	175
Start.....	175
Stop.....	175
PMCU.....	175
Attributes.....	175
PMCU.....	175
Physical.....	175
Temperature Sensor.....	176
Actions.....	176
Power Supply.....	176
Attributes.....	176
Power Supply.....	176
Physical.....	176
Logical.....	176
Actions.....	177
Replace.....	177
Replacement Guidelines and Precautions.....	177
Preparing to Replace the Power Supply.....	177
Removing the Power Supply.....	178
Installing the Replacement Power Supply.....	180
Power Supply (Blade Element).....	180

Attributes.....	180
Power Supply.....	180
Physical.....	181
Actions.....	181
Replace.....	181
Power Supply (CLIM).....	181
Attributes.....	181
Power Supply.....	181
Logical.....	181
Actions.....	181
Replace.....	181
Power Supply (FCDM).....	181
Attributes.....	182
Power Supply.....	182
Physical.....	182
Logical.....	182
Actions.....	182
Blink LED Off.....	182
Blink LED On.....	182
Replace.....	182
Power Supply (IOAM).....	182
Attributes.....	182
IOAM Power Supply.....	182
Physical.....	183
Logical.....	183
Configuration.....	183
Actions.....	183
Configure Power Source as AC.....	183
Configure Power Source as UPS.....	183
Delete the Power Source Configuration.....	184
Power Supply (Processor Switch).....	184
Attributes.....	184
Physical.....	184
Logical.....	184
Configuration.....	184
Actions.....	184
Configure Power Source as AC.....	184
Configure Power Source as UPS.....	184
Delete the Power Source Configuration.....	185
Replace.....	185
Set LED State.....	185
Power Supply (SAS Disk Enclosure).....	185
Attributes.....	185
Actions.....	185
Replace.....	185
Power Supply and Fan (Telco SAS Disk Enclosure).....	185
Attributes.....	185
Actions.....	185
Replace.....	185
Power Supply (VIO).....	185
Attributes.....	186
VIO Power Supply.....	186
Physical.....	186
Logical.....	186
Configuration.....	186

Actions.....	186
Configure Power Source as AC.....	186
Configure Power Source as UPS.....	186
Delete the Power Source Configuration.....	187
Replace.....	187
Processor (CLIM).....	187
Attributes.....	187
Processor.....	187
Physical.....	187
Logical.....	187
Actions.....	187
Replace.....	187
Processor Blade.....	187
Attributes.....	188
Processor Blade.....	188
Physical.....	188
Logical.....	188
Actions.....	188
Clear Forward Progress Log.....	188
Launch iLO URL.....	188
Replace.....	188
Retrieve and Clear BMC Event Log.....	188
Retrieve and Clear BMC Event Log - Formatted.....	188
Retrieve Forward Progress Log.....	189
Processor Components.....	189
Attributes.....	189
Processor Components.....	189
Physical Location.....	189
Processor Elements.....	189
LSU Logic Board.....	190
LSU Optics Adapter.....	191
Actions.....	191
Disable PE Reintegration.....	191
Disable Serial ZX1 I/O Link.....	191
Enable PE Reintegration.....	191
Enable Serial ZX1 I/O Link.....	191
Power Down LSU.....	191
Reintegrate PE.....	191
Replace LSU.....	191
Reset LSU.....	191
Set LED State.....	192
Set Physical Location.....	192
Stop PE.....	192
Take Dump On Next Failure.....	192
Processor Switch Module.....	192
Attributes.....	193
Physical.....	193
Physical Location.....	193
Actions.....	193
Read LCD.....	193
Rediscover.....	193
Replace.....	194
Retrieve Network Connectivity Info.....	194
Set Physical Location.....	194
Synchronize FIR Files to Other Switches.....	194

Write LCD Line.....	194
SAC (ServerNet Addressable Controller).....	194
Attributes.....	195
SAC.....	195
Physical.....	195
Logical.....	195
Firmware.....	196
Actions.....	196
Abort.....	196
Firmware Update.....	196
Responsive Test.....	196
Start.....	196
Stop.....	196
Test Verify.....	196
SAS Card (CLIM).....	196
Attributes.....	196
Physical.....	196
Logical.....	197
BIOS.....	197
Firmware.....	197
Actions.....	197
BIOS Update.....	197
Firmware Update.....	197
Replace.....	197
SAS Disk Enclosure.....	197
Attributes.....	198
SAS Disk Enclosure.....	198
Physical.....	198
Connected SAS Card-1.....	198
Connected SAS Card-2.....	198
Logical.....	198
Physical Location.....	198
Firmware.....	198
Actions.....	199
Firmware Update.....	199
Replace.....	199
Set LED State.....	199
SAS Disk Enclosures.....	199
Attributes.....	199
Actions.....	199
SCSI Controller.....	199
Attributes.....	199
SCSI Controller.....	199
Logical.....	199
Actions.....	200
Responsive Test.....	200
ServerNet Interface Card (Blade).....	200
Attributes.....	200
ServerNet Interface Card.....	200
Physical.....	200
Actions.....	200
Replace.....	200
ServerNet Interface Card (CLIM).....	200
Attributes.....	201
ServerNet Interface Card.....	201

Physical.....	201
Actions.....	201
Replace.....	201
ServerNet PIC.....	201
Attributes.....	201
Physical.....	201
Logical.....	201
Actions.....	202
Enable ServerNet Port.....	202
Power Off.....	202
Power On.....	202
Replace.....	202
Set LED State.....	202
ServerNet Port.....	202
Attributes.....	203
Logical.....	203
Actions.....	203
ServerNet Switch (Blade Enclosure).....	203
Attributes.....	203
ServerNet Switch.....	203
Physical.....	203
Logical.....	203
ME FPGA.....	204
ME Firmware.....	204
Actions.....	204
Dump Memory.....	204
Hard Reset.....	204
Launch Switch URL.....	204
ME FPGA Update.....	204
ME Firmware Update.....	204
Replace.....	204
Soft Reset.....	205
Synchronize FIR Files to Other Switches.....	205
ServerNet Switch Board.....	205
Attributes.....	205
ServerNet Switch Board.....	205
Physical.....	205
Logical.....	206
ME FPGA.....	206
ME Firmware.....	206
Actions.....	206
Dump Memory.....	206
Hard Reset.....	206
ME FPGA Update.....	206
ME Firmware Update.....	207
Power Cycle.....	207
Replace.....	207
Set LED State.....	207
Soft Reset.....	207
Service Processor (SP).....	207
Attributes.....	207
SP.....	207
Logical.....	207
SP Firmware.....	208
SCSI Boot Code Firmware.....	208

Processor Boot Millicode Firmware.....	208
Actions.....	209
Reset.....	209
Responsive Test.....	209
SP Firmware Update.....	209
Smart Array Controller (CLIM).....	209
Attributes.....	209
Smart Array Controller.....	209
Logical.....	209
Physical.....	209
Firmware.....	209
Actions.....	210
Firmware Update.....	210
SNDA (ServerNet/DA).....	210
Attributes.....	210
SNDA.....	210
Physical.....	210
Storage ASIC.....	210
Actions.....	210
Replace.....	210
Storage ASIC Initialization Test.....	211
Test Verify.....	211
SSAC (SCSI SAC).....	211
Attributes.....	211
SSAC.....	211
Physical.....	211
Logical.....	211
Actions.....	211
Responsive Test.....	211
Storage Router.....	211
Attributes.....	212
Storage Router.....	212
Logical.....	212
Physical.....	212
Process Pair.....	213
SCSI Interface.....	213
Actions.....	213
Responsive Test.....	213
Switch Process Pair.....	213
SWAN / SWAN2.....	213
Attributes.....	214
SWAN \$ZZWAN.....	214
Physical.....	214
Logical.....	214
Primary Host Connection.....	215
Alternate Host Connection.....	215
Actions.....	215
Start.....	215
Stop.....	215
Verify Logical Configuration.....	215
SWAN Battery.....	215
Attributes.....	216
Battery \$ZZWAN.....	216
Logical.....	216
Actions.....	216

SWAN CLIP.....	216
Attributes.....	216
CLIP \$ZZWAN.....	216
Logical.....	216
Physical.....	217
Firmware.....	217
Actions.....	217
Firmware Update.....	217
Start.....	217
Stop.....	217
Test Backup Path Access.....	217
Test Basic Online.....	217
Test Full Path Access.....	217
Test Primary Path Access.....	218
Test Verify.....	218
SWAN Collection.....	218
Attributes.....	218
Actions.....	218
SWAN FAN.....	218
Attributes.....	218
Fan \$ZZWAN.....	218
Logical.....	218
Actions.....	218
SWAN LAN Logic Board (LANLB).....	218
Attributes.....	219
LAN LB \$ZZWAN.....	219
Physical.....	219
Logical.....	219
Actions.....	219
SWAN Line.....	219
Attributes.....	219
Line \$ZZWAN.....	219
Logical.....	219
Actions.....	220
External Loopback Test.....	220
Start DLC Task.....	220
Stop DLC Task.....	220
SWAN Path.....	220
Attributes.....	220
PATH \$ZZWAN.....	220
Logical.....	220
Actions.....	220
Start.....	220
Stop.....	220
Verify Logical Configuration.....	221
SWAN (Power Supply).....	221
Attributes.....	221
Power Supply.....	221
Physical.....	221
Logical.....	221
Actions.....	221
System.....	221
Attributes.....	221
System.....	221
Logical.....	222

Operating System.....	222
Data Collection Services.....	222
System Load Configuration.....	222
Incident Report Configuration.....	223
Actions.....	223
Add Node to ServerNet Cluster.....	223
Bring Up and Balance Storage Paths.....	223
Check DHCP and DNS Server Status.....	223
Check Storage Dependence on ServerNet Fabric.....	223
Clear External BladeCluster Configuration.....	223
Collect Diagnostic Data.....	224
Compare HSS Firmware Versions	224
Copy Core License to Alternate System Disk.....	224
Delete System Load Configuration.....	224
Detect New Hardware.....	224
Enable/Disable Automation of Data Collection.....	224
Enable/Disable Blade Power Regulator Management.....	224
Extend Problem Incident Report Suppression Time.....	225
Get SMARTSSD Wear Status Summary.....	225
Initialize Default Firmware File Names.....	225
Install Core License File.....	226
Perform Data Sanitization.....	226
Read Core License.....	226
Rediscover System.....	226
Rediscover System and Cluster.....	226
Reinitialize Complex Manager.....	226
Set Data Collection Volume.....	227
Set Days to Persist for Diagnostic Data.....	227
Set System Type.....	227
Suppress Problem Incident Report Creation.....	227
Synchronize iLO Clocks to NonStop Clock.....	227
System Power Off.....	227
Test Incident Report Delivery Paths.....	227
Unsuppress Problem Incident Report Creation.....	228
Update Running Core License.....	228
Verify Power Fail Configuration.....	228
Related System and Processor-Level Recovery Actions.....	228
Tape Collection.....	228
Attributes.....	228
Actions.....	229
Tape.....	229
Attributes.....	229
Tape Drive.....	229
Logical.....	229
Physical.....	230
Process Pair.....	230
Controller Path.....	230
Associated Device.....	230
CLIM Path.....	231
Actions.....	231
Responsive Test.....	231
Start.....	231
Stop.....	231
Switch Process Pair.....	231
Test Extended.....	231

Test Verify.....	232
TRSA (Token Ring ServerNet Adapter).....	232
Attributes.....	232
TRSA.....	232
Physical.....	232
Logical.....	232
Actions.....	232
Abort.....	232
Start.....	232
Stop.....	233
Unknown CRU.....	233
Attributes.....	233
Unknown CRU.....	233
Physical.....	233
Actions.....	233
UPS.....	233
Attributes.....	233
UPS.....	233
Physical.....	233
Physical Location.....	234
Actions.....	234
Link to Web Interface.....	234
Rediscover.....	234
Stop Monitoring.....	234
VIO FCSA.....	234
Attributes.....	234
FCSA.....	234
Physical.....	235
Flash Firmware.....	235
Flash Boot Firmware.....	235
Actions.....	235
Flash Boot Firmware Update.....	235
Flash Firmware Update.....	235
Replace.....	235
Responsive Test.....	235
Test Verify.....	235
VIO G4SA.....	236
Attributes.....	236
G4SA.....	236
Physical.....	236
Logical.....	236
Actions.....	237
Abort.....	237
Add.....	237
Delete.....	237
Power Off.....	237
Replace.....	237
Reset.....	237
Start.....	237
Stop.....	237
VIO Logic Board.....	237
Attributes.....	237
VIO Logic Board.....	237
Physical.....	238
Logical.....	238

ME FPGA.....	238
ME Firmware.....	238
Actions.....	238
Dump Memory.....	238
Hard Reset.....	239
ME FPGA Update.....	239
ME Firmware Update.....	239
Power Cycle.....	239
Replace.....	239
Set LED State.....	239
Soft Reset.....	239
VIO Module.....	239
Attributes.....	240
VIO Module.....	240
Physical.....	241
Physical Location.....	241
Actions.....	241
Read LCD.....	241
Replace.....	241
Retrieve Network Connectivity Info.....	241
Set Physical Location.....	241
Synchronize FIR Files to Other Switches.....	242
Write LCD Line.....	242
Common Attribute Values.....	242
Battery Charge Status.....	242
Compare State (CLIM, SAS Disk Enclosure, CLIM SAS Card, and CLIM FC Card).....	242
Compare State (Other).....	243
Device State.....	243
Enabled State.....	243
Group Type.....	244
Path State.....	244
Power State.....	244
Processor State.....	245
Processor Type.....	245
Service State.....	246
Tape Types.....	247
Topology.....	248
12 Managing a ServerNet Cluster.....	249
BladeCluster Solution.....	249
Locating and Viewing Cluster Resources.....	249
Monitoring a Cluster.....	250
Performing Actions on Cluster Resources.....	250
Specifying a Cluster Switch Locator String.....	251
Updating Cluster Switches.....	251
Managing One of the Star Topologies With OSM.....	252
Router Connections in a Layered Topology.....	252
Router Connections for Switch Node Ports.....	252
Router Connections for Ports Connecting to Other Switches.....	252
Router Connections for Router Interconnect PICs.....	253
13 Cluster Resources.....	254
6770 Switch Module.....	254
Attributes.....	255
Switch Module.....	255
Logical.....	255

Actions.....	255
Replace.....	255
Set Locator.....	255
6780 Switch Module.....	255
Attributes.....	255
Switch Module.....	255
Midplane Physical.....	256
Logical.....	256
Temperature.....	256
Actions.....	256
Blink All LEDs Off.....	256
Blink All LEDs On.....	256
Connect to UPS.....	256
Replace.....	256
Responsive Test.....	257
Set Locator.....	257
AC Transfer Switch.....	257
Attributes.....	257
AC Transfer Switch.....	257
Logical.....	257
Actions.....	257
Replace.....	257
BladeCluster.....	257
Attributes.....	258
BladeCluster.....	258
BladeCluster Service.....	258
Logical.....	258
Actions.....	258
Place Local Node in Service.....	258
Reset ServerNet Statistics.....	258
ServerNet Path Test on X Fabric.....	258
ServerNet Path Test on Y Fabric.....	259
Set ServerNet Cluster State.....	259
External ServerNet Fabric.....	259
Attributes.....	259
External ServerNet X Fabric.....	259
Logical.....	259
Actions.....	259
Node Connectivity ServerNet Path Test.....	259
Local or Remote BladeCluster Node.....	259
Attributes.....	260
Logical.....	260
Expand_Over_ServerNet Configuration.....	260
Y Fabric Connection #1.....	260
Y Fabric Connection #2.....	261
X Fabric Connection #1.....	261
X Fabric Connection #2.....	261
Actions.....	261
Generate ServerNet Statistics	261
X Fabric Responsive Test.....	261
Y Fabric Responsive Test.....	261
Remote 6770 Switch.....	261
Attributes.....	261
Remote Switch.....	261
Physical.....	261

Actions.....	262
ServerNet Cluster.....	262
Attributes.....	262
ServerNet Cluster.....	262
Logical.....	262
ServerNet Cluster Service.....	262
SANMAN Process Pair.....	262
SNETMON Process Pair.....	263
Actions.....	263
Rediscover.....	263
Reset ServerNet Statistics.....	263
Set ServerNet Cluster State.....	263
Switch SANMAN Process Pair.....	263
Switch SNETMON Process Pair.....	263
Update Topology.....	263
ServerNet Local Node.....	264
Attributes.....	264
ServerNet Local Node.....	264
Logical.....	264
Actions.....	264
Generate ServerNet Statistics.....	264
ServerNet Remote Node.....	264
Attributes.....	264
ServerNet Remote Node.....	264
Logical.....	265
Expand-Over-ServerNet Configuration.....	265
Actions.....	265
Generate ServerNet Statistics.....	265
ServerNet II Switch.....	265
Attributes.....	266
Switch.....	266
Logical.....	266
Firmware.....	266
Configuration.....	266
Actions.....	266
Blink LED Off.....	266
Blink LED On.....	267
Configuration Update.....	267
Firmware Update.....	267
Hard Reset.....	267
Prepare to Replace.....	267
Replace.....	267
Set Fabric Setting.....	267
Soft Reset.....	267
Switch Fan.....	267
Attributes.....	268
Physical.....	268
Logical.....	268
Actions.....	268
Blink LED Off.....	268
Blink LED On.....	268
Switch Group.....	268
Attributes.....	268
Switch Group.....	268
Logical.....	268

Actions.....	269
Switch Logic Board.....	269
Attributes.....	269
Switch Logic Board.....	269
Physical.....	269
Logical.....	269
Firmware.....	269
Configuration.....	270
FPGA.....	270
Actions.....	270
Blink LED Off.....	270
Blink LED On.....	270
Configuration Update.....	270
Dump.....	270
Firmware Update.....	270
FPGA Update.....	271
Hard Reset.....	271
Replace.....	271
Soft Reset.....	271
Switch PIC.....	271
Attributes.....	271
Switch PIC.....	271
Physical.....	271
Logical.....	272
Actions.....	272
Blink LED Off.....	272
Blink LED On.....	272
Replace.....	272
Switch Power Supply.....	272
Attributes.....	272
Power Supply.....	272
Physical.....	272
Logical.....	272
Actions.....	273
Blink LED Off.....	273
Blink LED On.....	273
Switch-to-Node PIC.....	273
Attributes.....	273
Switch PIC.....	273
Logical.....	273
Neighbor ServerNet Node.....	273
Actions.....	274
Node Responsive Test.....	274
Switch Node Port.....	274
Attributes.....	274
Switch Node Port.....	274
Transceiver Physical.....	274
Logical.....	274
Neighbor ServerNet Node.....	275
Actions.....	275
Node Responsive Test.....	275
Switch-to-Switch PIC.....	275
Attributes.....	275
Switch PIC.....	275
Logical.....	275

Neighbor Switch PIC.....	276
Actions.....	276
Switch Port.....	276
Attributes.....	276
Switch Port.....	276
Transceiver Physical.....	276
Logical.....	276
Neighbor Switch Port.....	277
Actions.....	277
UPS (6770 Switch Module).....	277
Attributes.....	277
UPS.....	277
Physical.....	277
Logical.....	278
Actions.....	278
Replace.....	278
Common Attribute Values.....	278
Service State.....	278
Fabric State.....	278
Configuration Tag.....	278
Port Connectivity Status.....	279
14 Updating ServerNet Cluster Topology.....	280
Identifying Your Update Type.....	280
Migrating to the Layered Topology.....	280
Adding Layers or Zones to a Layered Topology.....	280
Updating Star Topologies.....	280
Software Requirements for Split-Star and Tri-Star Topologies.....	282
Cable Connections Between Star Groups.....	283
Updating to the Split-Star Topology.....	283
Updating to the Tri-Star Topology.....	283
Cable Connections in a Layered Topology.....	283
Connections Between Layers Within a Switch Group.....	283
X Fabric Connections Between Two Zones.....	284
Y Fabric Connections Between Two Zones.....	285
X Fabric Connections for Three Zones.....	285
Y Fabric Connections for Three Zones.....	286
Index.....	288
15 Register CLIMs with Key Managers Guided Procedure Online Help.....	295
Selecting CLIMs to Be Registered.....	295
Configuring a Key Manager Cluster.....	296
Creating CLIM Group, Username, and Password.....	298
Using the Select the Local CA Dialog Box.....	300
Selecting Certification Method and Creating Client Certificates.....	301
Creating Client Certificate Automatically.....	302
Use Your Own X.509 Certificate.....	303
Registering CLIMs.....	305

What's New in This Guide

Describes features available with OSM Service Connection version T0682 H02 ADL, including:

- Support/requirement for Java 7. For configuration steps necessary to use OSM with Java 7, see [Launching an OSM Service Connection](#) and [Enabling Java Next Generation Plug-in to Avoid OSM Memory Errors](#).

Java 7 also requires Windows Server 2003 Hotfixes in order to use OSM T0682 H02 ADL (and later) on Windows Server 2003. Those Hotfixes are available on NonStop System Console Installer DVD, Update 22 (and later). For information on installing those Windows Server 2003 Hotfixes, see the *NonStop System Console Installer Guide*.

The *OSM Configuration Guide* contains a troubleshooting tip for configuring Java 7 to avoid long delays in logging on to the OSM Service Connection on a private network.
- Support for Internet Explorer (IE) 9.0 (on Windows Server 2008) as well as support for using Internet Explorer 10.0 in compatibility mode only. For information on configuring IE to use either of those versions for OSM, see the *OSM Configuration Guide*.
- Default OSM certificates are now signed with SHA256 instead of SHA1. The SSL cipher suites for OSM Service Connection and Event Viewer include more advanced ciphers. For more information, see the *OSM Configuration Guide*.
- A new [Set UID LED State](#) action on the CLIM object to aid in the physical identification of a CLIM.
- Support for LTO-6 tape drives.
- The ability to specify a Rack Location value to help differentiate between the various racks displayed in the [Physical Configuration Tool](#).

Recent OSM History

This version of the OSM Service Connection (T0682 H02 ADH), released in conjunction with the H06.28/J06.17 RVUs, adds:

- Support for HP Integrity NonStop NS2300 servers and NS2400 series servers, including new [Processor Type](#) values of NSE-AG for NS2300 and NSE-AH for NS2400 series.
- Removed all occurrences of the Enable Memory Snapshot action, as it is not valid for H- and J-series systems.

This version of the OSM Service Connection (T0682 H02 ADF), released in conjunction with the H06.27/J06.16 RVUs, adds:

- Support for HP Integrity NonStop BladeSystem NB56000c and NonStop BladeSystem NB56000c-cg (Carrier Grade), including a [Processor Type](#) value of NSE-AF.
- [Get SMARTSSD Wear Status Summary](#) guided procedure on the system object.
- Support for [16-port Ethernet controllers \(G16SE\)](#) on all AC-powered NonStop BladeSystems except for NonStop BladeSystem NB50000c.
- OSMCONF flag options that allow you to disable all dial-outs and also the ability to specify alarms that should not be disabled from dialing out. For more information, see the *OSM Configuration Guide*.
- New alarm for hung Baseboard Management Controller (BMC) and iLO on processor blades in Integrity NonStop BladeSystems and blade elements in Integrity NonStop NS-Series servers.
- Ability to disable bouncing ServerNet links and create an alarm for them.
- OSM certificates now use SHA1 instead of MD5 (for more information, see the *OSM Configuration Guide*).

Also new for H06.27/J06.16, OSM Low-Level Link (T0633 G07 ABS) adds a “Select to change iLO **Admin** user's password” option in the Configure CLIM dialog box. This allows you to change this password without logging on to the iLO interface. If there is no **Admin** user ID yet – as may be the case with replacement CLIMs – this Low-Level Link action creates that **Admin** user ID and allows you to establish a password for it.

At H06.26/J06.15, OSM Service Connection (T0682 H02 ADD) added:

- Support for Gen8 CLIMs, including new attributes and/or attribute values on these CLIM subcomponent objects: [Hard Disk](#), [DIMM](#), [NIC](#), and [Smart Array Controller](#).
- Display of the Firmware Version attribute on the CLIM [Hard Disk](#) object for all CLIM types.
- Support for double chip sparing. For NonStop NB54000c, NS2200, and NS2100 servers, which have 4-bit wide DRAM devices, an alarm calling for DIMM replacement is not generated until two DRAM devices within the same rank fail, saving unnecessary service.
- Support for specifying a user other than the default NSC users (the Administrator, NSC_Administrator, and GCSC user accounts) when performing the [Prepare for Down System CLIM Firmware Update](#) action on the CLIMs object.
- For T0682 H02 ADD (and later), SSL is enabled for OSM by default for all H-series systems. Previously, this was the default for J-series systems only; for H-series systems, you had to enable SSL through an OSMCONF setting.

NOTE: The SSL support built into OSM relies on a “shared” SSL certificate. For maximum security, HP recommends that you generate a private SSL certificate, as described in the *OSM Configuration Guide*.

- Creation of a major alarm if a DP2 process for a disk volume enters a softdown state and the other processor is down and/or the other DP2 process is already softdown
- The OSM Event Viewer now allows you view events time-stamped in the same time zone as the system on which they were logged. For more information, see the OSM Event Viewer online help.
- The Register CLIMs with Key Managers Guided Procedure now supports 2048 bit certificates.
- Apache OpenOffice can be installed on NonStop system consoles as part of the OSM Console Tools product on NSC Installer DVD, Update 19 or later. It provides a method to view spreadsheets, documents, presentations on the system console; for example, files created by OSM in .csv (or comma delimited) format, such as hardware inventories created by the OSM System Inventory Tool, and Access Control List reports or saved Multi-Resource Views created in the OSM Service Connection.

At H06.25/J06.14, OSM Service Connection (T0682 H02 ACZ) added:

- Support for HP Integrity NonStop NS2100 servers, including a [Processor Type](#) value of NSE-AE, as displayed in that attribute of the [Logical Processor](#) object.
- A new guided procedure to make the replacement of CLIMs more automated can be launched through the [Replace](#) action on the [CLIM](#) object. A similar guided procedure for replacement of CLIM Hard Disk Drives can be launched either through the [Replace](#) action on the [CLIM Hard Disk](#) object or the [Replace Hard Drive](#) action on the [CLIM](#) object.
- Also new for the [CLIM](#) object, actions to [Backup](#) and [Restore](#) the CLIM configuration.
- A new [Enable/Disable Blade Power Regulator Management](#) action on the System object for HP Integrity NonStop NB54000c and NB54000c-CG BladeSystems. There are also two new related attributes under the Logical heading for the [System](#) object: Power Regulator Management Supported and Power Regulator Management Status.
- Support for Multiple Providers per CLIM, including an additional field in the [Configure CLIM](#) action where you indicate whether or not the CLIM will be configured to support multiple providers.

- A new [Place Local Node in Service](#) action on the BladeCluster object, to be used when intentionally halting a system to prevent all other directly-connected nodes from dialing out an alarm as soon as SNETMON is stopped or the node is halted.
- Support for analyzing the system board battery sensor in RX2620, RX2660, RX2800 i2, BL860c, and BL860c i2 servers at initial blade discovery and whenever the Save BMC Event Log is retrieved (the default interval is every 24 hours). Upon detecting a battery that does not meet performance requirements, OSM generates an alarm and dial-out to indicate that the battery needs to be replaced.
- Support for invoking the CLIM iLO through the [Invoke iLO](#) action on the [CLIM](#) object even when SNMP is not available. A new attribute on the CLIM object, iLO DNS Name, is also displayed whether or not SNMP is available.
- These new configuration options, which are enabled through OSMCONF parameters, as described in the *OSM Configuration Guide*:
 - Suppression of alarms based on a specific problem and resource name.
 - Support for having OSM bind to a specific IP address and TCP/IP stack, for OSM to use when sending indications to the OSM Service Connection, HP Systems Insight Manager or HP Insight Remote Support Advanced.

At H06.24/J06.13, OSM Service Connection (T0682 H02 ACV) added:

- Support for Core Licensing on HP Integrity NonStop NB54000c and NB54000c-CG BladeSystems, including four new actions on the [System](#) object, two new attributes on the [Logical Processor](#) object, and changes to the Save As System Load Configuration action on the [Disk](#), [Disk \(Fibre Channel\)](#), and [CLIM-Attached Disk](#) objects.
- Support for IPv6 (in addition to previous support for IPv4) on the operations and maintenance LANs, including an OSMCONF file setting. For more information, see the *OSM Configuration Guide*.
- [Collect CLIM Logs](#) action has been added to the CLIM object (was previously on just the CLIMs object).
- A new Prepare for Down System CLIM Firmware Update action on the [CLIMs](#) object, to be used in conjunction with the Down System CLIM Firmware Update Tool, a new component of OSM Console Tools T0634 G06 ABB and later.

OSM Console Tools T0634 G06 ABB and later also includes the NonStop Maintenance LAN DHCP DNS Configuration Wizard, which replaces the CLIM Boot Service Configuration Wizard. It can be used to configure the DHCP and DNS servers required for NonStop J-series systems and any NonStop systems with CLIMs attached.

For information on installing OSM Console Tools components, see the *NonStop System Console Installer Guide*. For information on using the NonStop Maintenance LAN DHCP DNS Configuration Wizard or the Down System CLIM Firmware Update Tool, see the online help available from within those tools.

At H06.23/J06.12, OSM Service Connection (T0682 H02 ACN) added:

- Support for HP Integrity NonStop NS2200 series servers, including the new [Processor Type](#) value of NSE-AD, as displayed in that attribute of the [Logical Processor](#) object.
- Support for Solid State Drives (SSDs) in D2700 Enclosures, including:
 - A [Show SMARTSSD Wear Gauge](#) action has been added to the [SAS Disk](#) object.
 - A Media Type attribute has been added to the [SAS Disk](#) object to indicate whether the disk is Magnetic or Solid State.

- Support for disk partitioning on both Hard Disk Drives (HDDs) and Solid State Disks (SDDs), including:
 - The Start Disk, Start Volume, Stop Disk, and Get Logical Disk(s) actions on the [SAS Disk](#) object have been modified to work with partitioned disks.
 - A Partition Number attribute has been added to the [CLIM-Attached Disk](#) object to indicate the partition number.
- For G6 [CLIMs](#), a new subcomponent [InfiniBand HCA Card](#) object.
- Support for collecting CLIM logs onto a NonStop system, through two new actions on the [CLIMs](#) object: [Collect CLIM Logs](#) and [Set Location for CLIM Log Collection](#).
- Support for enhanced [BladeCluster Solution](#) options.

At H06.22/J06.11, OSM Service Connection (T0682 H02 ACJ) added:

- Support for Integrity NonStop NB54000 BladeSystems.
- The ability to control access to certain OSM Service Connection actions through the [Access Control List](#) feature.
- The option of having Up-rev firmware on CLIM and SAS Disk Enclosure components flagged as a problem attribute that is propagated up to parent objects in the OSM Service Connection. For information on how configure this option in your OSMCONF file, see the *OSM Configuration Guide*.
- The option of configuring OSM to monitor system devices (storage routers, UPSs, maintenance switches, Onboard Administrators, or CLIMs) located outside of the dedicated service LAN. For information on how configure this feature in your OSMCONF file, see the *OSM Configuration Guide*.
- A Start Volume action has been added to the [SAS Disk](#) object.
- A Set LED State action has been added to the [CLIM-Attached Disk](#) object.

At H06.21/J06.10, OSM Service Connection (T0682 H02 ACE) added support for:

- G6 CLIMs, including the display of two new subcomponent objects in the OSM Service Connection, [Motherboard](#) and [Smart Array Controller](#), as well as some changes to these existing [CLIM](#) subcomponents:
 - [DIMM](#)
 - [Hard Disk](#)
 - [PCI Riser](#)
 - [SAS Card](#)
- You can now specify an optional process priority for the **Validate Checksum** and **Clear Data** actions that are available under supported disk types.
- New [Display Diagnostic Status Errors](#) action on the [Enclosure](#) object.
- New [Compare HSS Firmware Versions](#) action on the [System](#) object.

At H06.20/J06.09, OSM Service Connection (T0682 H02 ACC) added support for:

- NonStop Volume Level Encryption, which provides a simple and secure method for registering CLIMs with Enterprise Secure Key Managers. OSM support includes:
 - A new guided procedure, launched from an action on the CLIMs (container) object, to help you [Register CLIMs with Key Managers](#).
 - A new action on individual CLIM objects to [Show CLIM/Key Manager Registration Information](#).
 - A new attribute on supported storage CLIM objects to indicate whether or not the CLIM has been [Registered with Key Managers](#).

NOTE: For more information on volume level encryption, including requirements and steps that must be taken before using the OSM guided procedure, see the *NonStop Volume Level Encryption Guide*.

- Using HP Insight Remote Support Advanced on multiple Central Management Servers (CMSs) to provide fault tolerance for remote support of NonStop NS-series systems and NonStop BladeSystems. For more information, see *Insight Remote Support Advanced for NonStop*, located in the Support and Service collection of the NonStop Technical Library.
- [BladeCluster Solution](#) enhancements, including support for two multi-zone topologies, interzone long-haul Dense Wavelength Division Multiplexing (DWDM) up to 25 kilometers (15.53 miles), and short-haul up to 125 meters (410 feet).
- A new "Compatible" attribute value for the Firmware Compare State on the [CLIM](#), [SAS Disk Enclosure](#), [CLIM SAS Card](#), and [CLIM FC Card](#) objects. This value indicates that the current firmware version running on the device is compatible with the firmware version file on the NonStop system, even though the firmware version on the device and the version of the firmware file are not exactly the same.

OSM also now includes VPROC information in the Default File Version attribute for those objects and the [CLIM NIC](#) object.

- An enhancement to the [Firmware Update action on SAS Disk Enclosure](#). Upon successful completion, OSM now gives you the option of turning on the enclosure's LED, to help you identify the enclosure for the purpose of power cycling it to complete the firmware update process.
- Additional attributes under the [Maintenance Switch](#) object to support the HP ProCurve 2510 Switch. While there is no Part Number attribute displayed for this switch, there are new Model and Configured System Name attributes to provide the necessary information.
- A new action, for HP Integrity NonStop NS16000 and NS14000 series servers only, called [Reclaim Memory Pages](#), located under the Logical Processor object.
- Requests for automated application system shutdown in the event of a power failure through two new OSMCONF variables, SHUTDOWN_SCRIPT_NAME and SHUTDOWN_SCRIPT_TIME. See the OSMINIO file for examples, and the *OSM Configuration Guide* for more information on creating or editing a customized OSMCONF file. The [Verify Power Fail Configuration](#) action on the System object now checks the validity of these two variables.
- Onboard Administrator firmware version is now displayed for NonStop BladeSystem [Enclosures](#) as Bay 1 and Bay 2 OA Firmware Version attributes, located under Logical attributes.
- When establishing an [OSM Service Connection session](#), OSM checks and informs you when a server certificate for Secure Sockets Layer (SSL) does not meet all requirements for establishing the trust relationship between the system console and the NonStop server.

At H06.19/J06.08, OSM Service Connection (T0682 H02 ABX) added:

- New actions on the System object to [Configure BladeCluster](#) and [Clear External Cluster Configuration](#).
- Support for new actions on the [Processor Blade](#) (BladeSystem) and [Blade Element](#) objects to clear or retrieve the Forward Progress Log.
- The [Reboot](#) action on the CLIM object has been enhanced, providing the option to perform a dump of diagnostic data before rebooting the CLIM.
- Persistence of [alarm suppression](#) and [problem attribute suppression](#), across OSM server sessions. To disable this feature, which is enabled by default in OSM T0682 H02 ABX and later, see the *OSM Configuration Guide*.
- Support for HP Insight Remote Support Advanced, including an action to [Test Incident Report Delivery Paths](#). For more information, see the *Insight Remote Support Advanced for NonStop*, located in the Support and Service collection of NTL.
- The online help version of the *OSM Service Connection User's Guide* has been converted to a JavaHelp interface that allows direct access from the [Help menu](#) of the OSM menu bar, rather than having to first download the entire help file. (As always, a PDF version is also available from the NonStop Technical Library at docs.hp.com.)

At H06.18/J06.07, OSM Service Connection (T0682 H02 ABU) added:

- Support for connecting CLuster I/O Modules (CLIMs) to Telco HP Integrity NonStop NS16000 series systems.
Some attributes names displayed in the OSM Service Connection for [CLIM](#) and [SAS Disk Enclosure](#) objects have changed.
- Support for [BladeCluster Solution](#).
The OSM Low-Level Link has also been updated to support BladeCluster Solution. For more information, see the OSM Low-Level Link online help.
- A new space-saving look for the [OSM menu bar](#).
- T0682 ABU also includes a configurable automatic log off security feature in the OSM Event Viewer. For more information, see the *OSM Configuration Guide*.

At H06.17/J06.06, the OSM Service Connection (T0682 H02 ABR) added:

- Support for HP Integrity NonStop NS2000 series servers.
- Support for the OSM Data Sanitization Guided Procedure, which is launched from the Perform Data Sanitization action under the [System](#) object.

At H06.16/J06.05, the OSM Service Connection (T0682 H02 ABP) added:

- Support for connecting CLuster I/O Modules ([CLIMs](#)) to HP Integrity NonStop NS16000 series systems.
- Additional support for Telco [Alarm Panels](#), including an action to [Start Monitoring Alarm Panel](#) under the [Monitored Service LAN Devices](#) object.

At H06.15/J06.04, the OSM Service Connection (T0682 H02 ABN) added support for HP Integrity NonStop BladeSystems in a Telco environment, including a [SAS Power Supply and Fan](#) object specific to Telco BladeSystems. For more information on Telco BladeSystems, see the *NonStop Carrier Grade BladeSystem Server Manual*

At H06.14/J06.03, the OSM Service Connection (T0682 H02 ABI) added support for J-series in addition to H-series RVUs. This version of the *OSM Service Connection User's Guide* was updated

to include support for J06.03 and the components, as displayed by the OSM Service Connection, of an HP Integrity NonStop BladeSystem, including:

- HP BladeSystem c-Class [Enclosure](#)
- CLuster I/O Module ([CLIM](#))
- [SAS Disk Enclosure](#)

For more information, see:

- *NonStop BladeSystems Planning Guide*
- *NonStop BladeSystems Hardware Installation Manual*
- *CLuster I/O Module (CLIM) Installation and Support Guide*
- *Common IP (CIP) Installation, Configuration, and Management Manual*

At H06.13, the OSM Service Connection Suite (T0682 H02 ABH) was updated to add support for:

- HP Integrity NonStop NS14200 systems, including changes to the [Initialize Default Firmware File Names](#) action to set the appropriate blade firmware information for NS14200 servers.
- [VIO Modules](#) used to provide a Versatile Ethernet ServerNet enclosure with 4 (V4SE) or 8 (V8SE) Gigabit Ethernet ports for NS16000CG and NS5000 (Telco) systems.

At H06.12, the OSM Service Connection Suite (T0682 H02 ABE) was updated to add support for:

- HP Integrity NonStop NS1200 servers
- A system-level [Initialize Default Firmware File Names](#) action to set the appropriate blade firmware information for NonStop NS16200 servers. For H06.12 and later, there are multiple versions of blade firmware on the SUT for NonStop NS14000 series and NS16000 series servers. This action is necessary in order for OSM to display the appropriate blade firmware information for NS16200 and NS16000/NS16200 hybrid systems.
- A [Reinitialize Complex Manager](#) action, used only in cooperation with your service provider, to reinitialize the Complex Manager Auxiliary Process (CMAP) for each processor in an Integrity NonStop NS14000 or NS16000 series server.
- An enhanced version 3 algorithm for the [Redundant Power Scrub](#) action on legacy (S-series) modules.

At H06.10, the OSM Service Connection Suite (T0682 H02 AAZ) was updated to add support for HP Integrity NonStop NS3000AC servers.

At H06.09, the OSM Service Connection Suite (T0682 H02 AAY) was updated to provide:

- Support for additional [Blade Element](#) components for HP Integrity NonStop NS1000 and NS5000 servers.
- Changes to the logon interface for the OSM actions to [Start Monitoring Maintenance Switch](#) and to [Start Monitoring UPS](#).

At H06.08, the OSM Service Connection Suite (T0682 H02 AAW) was updated to provide support for HP Integrity NonStop NS14000 and NS1000 servers containing VIO enclosures (represented in the OSM Service Connection as [VIO modules](#)).

Also for H06.08, the OSM Low-Level Link was updated to T0633 AAQ to provide support for VIO enclosures and add the ability to save (and use) system configurations on the system console. For more information, see the OSM Low-Level Link online help.

At H06.07, the OSM Service Connection Suite was updated to T0682 H02 AAU to provide support for:

- An improved module-level [Redundant Power Scrub](#) test. (Click the link or see softdoc for details.)
- RoHS-compliant hardware.
- Monitoring four [Blade Element](#) fans for Integrity NonStop NS1000 servers, five Blade Element fans for Integrity NonStop NS5000T and NS5000CG servers.

Also new for H06.07 is the OSM System Inventory Tool. Installed on your system console as part of client-based OSM Console Tools, T0634AAL or later, this tool can be used to create a hardware or firmware inventory file of one or more NonStop systems running OSM. The resulting file can be saved in .csv (or comma delimited) format for use in Microsoft Excel.

After installation, the OSM System Inventory Tool is launched from:

Select Start > Programs > HP OSM > OSM System Inventory Tool

For information on using the OSM System Inventory Tool, see the online help available from within the application.

At H06.06, the OSM Service Connection Suite was updated to T0682 H02 AAP. Changes included:

- Support for Integrity NonStop NS1000 and NS5000 servers.
- New system-level guided procedures, [Check Storage Dependence on ServerNet Fabric](#) and [Bring Up and Balance Storage Paths](#), to help you prepare for and recover from activities that disrupt ServerNet traffic on one fabric.

About This Guide

The *OSM Service Connection User's Guide* is available as online help within the OSM Service Connection, and in the NonStop Technical Library.

From within the OSM Service Connection, you can:

- Access a JavaHelp online help interface to the *OSM Service Connection User's Guide* by selecting **Help > Help Contents** from the OSM menu bar.
- Get a context-sensitive help topic (from the same JavaHelp interface) by selecting a system resource object, action, or OSM management window area and pressing the F1 key. Help is also available from many dialog box Help buttons.

Related Reading

Sources of OSM-related information:

- This manual, the *OSM Service Connection User's Guide*, is available in the NonStop Technical Library (NTL) and as online help from within the OSM Service Connection. It deals mostly with using the OSM Service Connection to monitor and perform actions on system and cluster resources.
- The Hardware Installation Manual for your NonStop system type, available in the Hardware Service and Maintenance collection of NTL, describes how to connect and configure a system console for use with OSM software and how to configure server components to allow communication with OSM.
- The *NonStop System Console Installer Guide* describes how to install OSM client-based components and other required system console software.
- The T0682 softdoc covers installation of the server-based component, along with a current list of fixes and known problems.
- The *OSM Configuration Guide* describes OSM requirements, explains how to configure and start OSM server processes, and provides an overview of the individual OSM applications.
- The *NonStop Operations Guide* documents using OSM for day-to-day monitoring and for recovery functions, such as reloading and dumping processors.
- The *H06.nn* or *J06.nn* *Software Installation and Upgrade Guide* documents procedures for using OSM to upgrade certain system component firmware.
- Online help is also available from within each of these OSM applications:
 - OSM Low-Level Link
 - OSM Event Viewer
 - OSM System Inventory Tool
 - OSM Certificate Tool
 - CLIM Boot Service Configuration Wizard
- Many OSM service actions launch guided procedures (which contain their own online help) or help topics to guide service providers (or in some case qualified operators) through replacement procedures. A complete repository for all service procedures (some also available in OSM, some not) can be found in the Support and Service collection of NTL.

1 Introducing OSM

The OSM client components are installed on a PC workstation that serves as the system console. The OSM server components are installed on the NonStop server running the HP NonStop operating system.

Server-Based Components

OSM server-based components (including the OSM Service Connection and OSM Event Viewer applications) have been combined into a single product, T0682.

For information on how to configure and start OSM server-based processes, see the *OSM Configuration Guide*.

Client-Based Components

T0633 – OSM Low-Level Link – Down-system support

T0634 – OSM Console Tools – Start menu shortcuts and default home pages for easy access to the OSM Service Connection and OSM Event Viewer (browser-based OSM applications that are not installed on the system console)

CAUTION: Only system consoles provided by HP are supported for use with the OSM applications. To preserve the integrity of software running on system consoles, do not install any software applications on your system consoles other than the preinstalled software. Compromising the software on a system console might leave you unable to communicate with the server when it is down.

For additional information, see [Related Reading](#).

OSM Interfaces

OSM Service Connection

The OSM Service Connection is the primary OSM management component. You use the OSM Service Connection to log on and establish a connection with a NonStop server. From the Management window, you can manage the resources of your server. If your server is part of a ServerNet cluster, you can also manage cluster resources.

OSM Guided Procedures

Guided procedures are launched by OSM actions:

OSM Guided Procedure	OSM Action	For Object
Replace IOMF or SNDA	Replace	IOMF or SNDA CRUs
Replace Switch II Component	Replace	HP NonStop Cluster Switch (model 6770) and subcomponents (UPS and AC transfer switch)
Replace 6780 Switch	Replace	HP NonStop ServerNet Switch (model 6780) and subcomponents (logic board and PIC)
Replace ServerNet Switch Board or IOAM Enclosure	For the IOAM Enclosure, the action is Replace IOAM Enclosure or ServerNet Switch Board. For the ServerNet Switch Board, the action is Replace.	IOAM Enclosure and ServerNet Switch Board
Add Node to ServerNet Cluster	Add Node to ServerNet Cluster	System

OSM Guided Procedure	OSM Action	For Object
Replace Fibre Channel Disk Module (FCDM) component	Replace	FCDM or subcomponent (Fibre Channel disk drive, FC-AL I/O module, EMU, power supply, and blower)
Replace Processor Switch component	Replace	Processor Switch or subcomponent (ServerNet Switch Board, Maintenance PIC, ServerNet PIC, fan, and power supply)
Replace Blade Element component	Replace	NonStop Blade Element or subcomponent (processor board, front panel display, memory board, reintegration board, fan, optics adapter, and I/O interface board)
Replace LSU	Replace LSU (located under Processor Components object)	LSU or subcomponent
Blade Complex Firmware Update	Firmware Update	Firmware running on each Blade Element in the Blade Complex
* NonStop NS-series only – should be performed only by a trained service provider. ** Should be performed only by a trained service provider.		

NOTE: You must be logged on as a super-group user to perform OSM guided procedures. You can minimize the OSM Service Connection Management window, but must not close it. If the session you launched the guided procedure from is closed or becomes disconnected, the guided procedure will close and fail to complete.

OSM Low-Level Link

The OSM Low-Level Link enables you to communicate with a server even when the NonStop Kernel operating system is not running. Also, some actions that are performed on a running server, such as starting the system or priming a processor for reload, require you to use the OSM Low-Level Link.

The OSM Low-Level Link can be installed and used only if you select the dedicated service LAN option during OSM client installation.

To start the OSM Low-Level Link, select **Start > Programs > HP OSM > OSM Low-Level Link**.

OSM Event Viewer

The OSM Event Viewer allows you to retrieve, view, and save EMS events from event logs. It also gives you access event details such as cause, effect, and recovery information.

The OSM Event Viewer is a browser-based application, closer in appearance and function to WebViewPoint than to the TSM EMS Event Viewer.

To start the OSM Event Viewer, select **Start > Programs > HP OSM > OSM Event Viewer**. You can also launch the OSM Event Viewer from within the OSM Service Connection by selecting Event Viewer from the OSM Tools menu.

2 Preparing the OSM Environment

To plan your network LAN configuration and connect your system console so it can communicate with your NonStop server through OSM client/server software, see the *NonStop NS-Series Hardware Installation Manual* (shipped with every new system; also available in the Hardware Service and Maintenance collection of NTL).

The *OSM Configuration Guide* describes how to configure and start OSM server-side processes.

The NonStop System Console Installer CD includes the client software required for OSM use. (The OSM Service Connection and OSM Event Viewer are server-based components, accessed through a browser session from the console or any qualified PC.) To install the OSM client components and other required software, see the *NonStop System Console Installer Guide*.

Installing OSM Components

System Console-Based Components

The *NonStop System Console Installer Guide*, available in NTL and provided in hard copy with the NonStop System Console Installer CD, describes how to install the OSM client components and other required HP and third-party software.

Server-Based Components

Installation of server-based OSM components is documented in the T0682 softdoc. The *OSM Configuration Guide* lists all server-based OSM components (combined into T0682) and describes how to configure and start OSM server-side processes.

Using OSM in Conjunction with HP SIM

HP Systems Insight Manager (SIM), which provides infrastructure management for all HP servers and storage, now supports the NonStop platform via a Web-Based Enterprise Management (WBEM) provided by OSM. HP SIM is capable of discovering NonStop systems, displaying and forwarding alarms generated by OSM, and collecting system and device data. Sources of information regarding HP SIM include:

- Whether or not HP SIM is right for your environment – HP SIM provides different values to different customer environments. Before installing HP SIM on your system console, see Support Note S05135 for information on the usage model of HP SIM for different customer environments.
- Installing the HP SIM client – Starting with Update 7, the NonStop System Console Installer kit (S7X-SWV1/HNSC-SWV1) includes an HP SIM CD from which you can install HP SIM. For hardware and software requirements and installation information, see the *NonStop System Console Installer Guide*.
- Configuration – Before using HP SIM in the NonStop environment, you must enable secure sockets layer (SSL) support in OSM. For more information, see the *OSM Configuration Guide*.

3 Configuring OSM

Before using OSM applications to manage your system.

- Configure the server using the OSM Low-Level Link (see [Configuring the Server](#)).
- If using HP Insight Remote Support Advanced for remote support services, see *Insight Remote Support Advanced for NonStop*, located in the external NonStop Service Information collection of NTL.
- [Configure OSM to Avoid Java Memory Errors](#)

NOTE: It is possible to start and run a new server without performing OSM configuration. However, HP strongly recommends that you perform OSM configuration tasks shortly after installing a new system. If you do not perform OSM configuration, your system will have certain user, security, and network limitations.

You can also change many OSM default settings by creating and using an OSMCONF file from the OSMINI template. For information on these configurable parameters and how to make OSMCONF changes take effect, see the *OSM Configuration Guide*.

Enabling Java Next Generation Plug-in to Avoid OSM Memory Errors

When logging on to OSM Service Connection version T0682 H02 ADL and later, if OSM detects that Java next generation plug-in is disabled, a pop-up dialog directs you to enable Java next generation plug-in, as appropriate, so that the required memory settings can take effect automatically:

- When using Internet Explorer 8.0 or 9.0, Java next generation plug-in should be enabled, per the instructions that follow.
- When using Internet Explorer 10.0 (supported in compatibility mode only), Java next generation plug-in must remain disabled.

NOTE: If OSM (T0682 H02 ADL and later) detects that Java next generation plug-in is already enabled, you will not be prompted to disable it, but must do so to establish an OSM Service Connection session with IE 10.

To enable Java next generation plug-in:

1. From the Windows Start menu, open Java Control Panel by the method appropriate for your console:
 - For Windows Server 2008, select **Control Panel > Programs > Java (32-bit)**
 - For Windows Server 2003, select **Control Panel > Java**
2. In the Java Control Panel, click on the **Advanced tab**.
3. Under Java Plug-in, place a check mark in the box next to "Enable the next-generation Java Plug-in."
4. Click **OK**, and close all Internet Explorer windows before reconnecting to the OSM Service Connection.

NOTE: When using older OSM versions (that require Java 6) on the same console, you will be instructed to disable next generation plug-in.

Configuring the Server

You must configure these server components using the OSM Low-Level Link:

Use this dialog box	To
Network	Configure unique MSP IP addresses for your primary and backup LANs.
Startup Windows	Define the workstations authorized to display the startup TACL prompt and receive the event messages that occur during a system load.
MSP Users	Define the users that are authorized to connect to the master service processors (MSPs) or maintenance entities (MEs) on your server. MSP users have access to your server using the OSM Low-Level Link only and are not user names for the OSM Service Connection.

Defining Users

To use the OSM client and server software, you must define the users that have access to your server. OSM allows two types of users:

MSP (Low-Level-Link) Users

- Can log on to the OSM Low-Level Link and connect to the MSP or ME, allowing them to access a server even when the NonStop operating system is not running.
- Have full privileges and can perform serious actions such as loading the processor or starting the system. Any MSP user can perform any action available in the OSM Low-Level Link.
- Have an MSP user name and password. You assign and modify MSP user names and passwords using the OSM Low-Level Link. OSM provides one predefined MSP user name, root. There is no predefined password for the root user. For security reasons, you should immediately specify a root password. For more information, see the OSM Low-Level Link online help.

NonStop Operating System Users

- Can connect to the server using the OSM Service Connection.
- Can perform OSM Service Connection tasks. Only super-group users (255,n) can initiate actions. Other users can log on and perform discovery but can perform only actions that verify the presence of a resource.
- Can access the OSM Event Viewer.
- Have a NonStop operating system user name and password. These user names and passwords are defined when you initialize your new system.

How to Plan Your Users

1. Define the general actions each person or group of persons will perform using the OSM software package.
2. Using the OSM Low-Level Link, define the MSP user names and passwords you will use. For more information about defining user names and passwords, see the OSM Low-Level Link online help.

Configuring OSM Power-Fail Support

HP Integrity NonStop NS-series systems do not have backup battery units; however, you can use a site or rack-integrated Uninterruptible power supply (UPS) unit to provide backup power in the event of a power failure.

For rack-integrated UPS units, OSM provides an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS. To configure this OSM power-fail support:

- For an HP Integrity NonStop NS16000 server, you must use the [Configure Power Source as UPS](#) action for at least one processor switch power supply unit to tell OSM that a rack-integrated UPS is configured to provide backup power.
- For an HP Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, or NS14000 series server, you must use the Configure Power Source as UPS action for at least one [IOAM power supply](#) or [VIO power supply](#) unit to tell OSM that a rack-integrated UPS is configured to provide backup power.
- For an HP Integrity NonStop Blades System, you must use the Configure a Power Source as UPS action for at least one power supply from the [Enclosure](#) object to tell OSM that a rack-integrated UPS is configured to provide backup power.

4 Starting the OSM Service Connection

You can:

- [Launch an OSM Service Connection](#)
- [OSM Service Connection Session Error Messages](#)
- [Using OSM Bookmarks](#)
- [Verify the OSM Service Connection State](#)
- [Run Multiple Sessions](#)

Launching an OSM Service Connection

NOTE: There are conditional requirements for using T0682 H02 ADL (and later), depending on how the Service Connection is being accessed:

- Because it uses Java 7, Windows Server 2003 Hotfixes are required in order to use OSM T0682 H02 ADL (and later) on Windows Server 2003. Those Hotfixes are available on NonStop System Console Installer DVD, Update 22 (and later). For information on installing those Windows Server 2003 Hotfixes, see the *NonStop System Console Installer Guide*.
- When using Internet Explorer 9.0 or 10.0 (supported in compatibility mode only) from a PC other than a NonStop system console, you may need to add the IP address or DNS name of NonStop system to the Trusted Sites of Internet Explorer, as described in the *OSM Configuration Guide*.

1. To initiate an OSM Service Connection session, either:
 - Open a new Internet Explorer browser window (but not from within a current browser window). In the Internet Explorer Address box, enter a system URL:
http://system_IP_address:9990
(example: http://155.155.155.155:9990)
http://system_host_name:9990
(example: http://himaxb.cac.cpqcorp.net:9990)
 - If OSM Console Tools is installed on your PC and you have an existing OSM system list or have saved your own OSM bookmarks previously (as described in [Using OSM Bookmarks](#))
 - a. From the Start menu, select:
Start > Programs > HP OSM > OSM Service Connection
 - b. In the left column of the home page, select a bookmark for the system you want to access.
2. If not already installed, OSM T0682 H02 ADL (and later) will prompt you to install Java 7 when you try to establish a service connection. Download it according to the instructions, then close the current browser, open a new one, and repeat Step 1.
3. With T0682 H02 ADL and later, a Security Warning is displayed, showing a Publisher name of "Hewlett-Packard" and a Location, which should be the domain name or IP address of the NonStop system. Click the check box next to "I accept the risk and want to run this application," then click **Run**.
4. If OSM detects that Java Next Generation Plug-in is disabled, it will direct you to instructions for [Enabling Java Next Generation Plug-in to Avoid OSM Memory Errors](#).
5. Upon satisfying the Java Runtime Environment requirements, a Log On dialog box prompts you for a valid username and password.

NOTE: When using Secure Sockets Layer (SSL) to establish a secure connection to the NonStop server, OSM checks that the server certificate that meets all requirements for establishing this trust relationship. If one or more of the requirements are not met, OSM displays a dialog box right after you submit logon credentials. This dialog box informs you that there is a problem with the OSM server certificate and lists the specific reason(s) for the problem. You have the option of exiting at this point, so you can fix the problem before establishing the connection, or continuing on to establish the connection despite the problem.

For more information on configuring SSL for OSM, and for generating a private SSL certificate that meets all requirements, see the *OSM Configuration Guide*.

6. The OSM Service Connection launches in a secondary window (to avoid displaying the standard Internet Explorer toolbar, which has features incompatible with OSM sessions). The initial window displays the message "You may now close this window."

OSM Service Connection Session Error Messages

Server Undiscovered

An OSM Service Connection session cannot be established until system discovery is complete. Close the browser session that generated the "Server Undiscovered" message, wait until discovery is complete and then establish a new OSM Service Connection session.

Server Down

An OSM Service Connection session cannot be established. There is either a communication problem between the console and the NonStop server, or \$ZCMOM and \$ZOSM processes are not running. Check the two processes and the LAN network that connects the console and the server. Once the problem has been resolved and system discovery is complete, open a new browser window and establish a new OSM Service Connection session.

Using OSM Bookmarks

You can create your own bookmarks for future use from within the OSM Service Connection. Once you are logged on to a system, select **Tools > Create Bookmark**. If you save the bookmark to the OSM Service Connection folder automatically created in your IE Favorites directory, these bookmarks also appear on the OSM Service Connection home page the next time you launch it.

Verifying the OSM Service Connection State

Select **Connection Status** from the [Summary menu](#). The Connection Status dialog box indicates the current state of all service connection processes. Each IP address listed is associated with a TCP/IP stack configured in the OSMCONF (OSM server configuration) file. OSM runs as a process pair for fault tolerance, which means the configuration file has two stacks configured by default. You must have at least two connections with a status of UP for your OSM Service Connection session to be fault tolerant.

Before bringing down either processor 0 or 1, it is important to know the state of your service connection on the other processor, so you do not lose your OSM Service Connection session.

For more information on LAN connectivity options and configuring more TCPIP stacks in the OSMCONF for additional fault tolerance, see the *OSM Configuration Guide*.

Running Multiple Sessions

You can run multiple sessions by:

Using either of the methods described in [Launching an OSM Service Connection](#)

You cannot run multiple sessions by:

- Reusing a browser window used for a previous OSM Service Connection session
- Selecting **File > New** to open a new OSM session from within an existing session

5 Using the Management Window

The [OSM Management window](#) appears after system discovery. It displays OSM features and information about your local system and ServerNet cluster. The Management window contains an [OSM menu bar](#) and these panes:

Overview	Displays a high-level view of system objects, such as internal fabrics, groups, and external devices (external disks and tapes), and of ServerNet Cluster objects, such as external fabrics, local nodes, and remote nodes.
Tree	Displays both system and cluster resources at the same time.
View	<p>Allows you to choose a view of the cluster or system:</p> <ul style="list-style-type: none">• Select Physical from the view drop-down list to display a physical view.• Select Inventory from the view drop-down list to display an inventory view. <p>The view pane toolbar displays both System Status and Logical Status icons to help indicate, at a glance, degraded conditions within the system and the components included in the Logical Status view.</p> <p>The inventory view also contains a Save button.</p>
Details	Provides Alarms and Attributes tabs to view specific information about the resource you selected in the overview, tree, or view pane.

The view and tree panes show the relationship between the location of a resource and its position in the hierarchy of the server or cluster. For example, when you select an IOAM Enclosure in the view pane, the IOAM Enclosure is automatically selected in the tree pane. Attributes and any alarms for the IOAM Enclosure appear in the details pane.

To display different views of the server at one time, launch additional browsers and select a different view in each one.

If the status of a resource is abnormal, the OSM Service Connection displays an icon or color over that resource. For more information, see [Interpreting Icons and Color](#). If a service processor cannot identify a system resource, that resource is represented by an Unknown CRU object in the tree pane featuring a blue question mark icon.

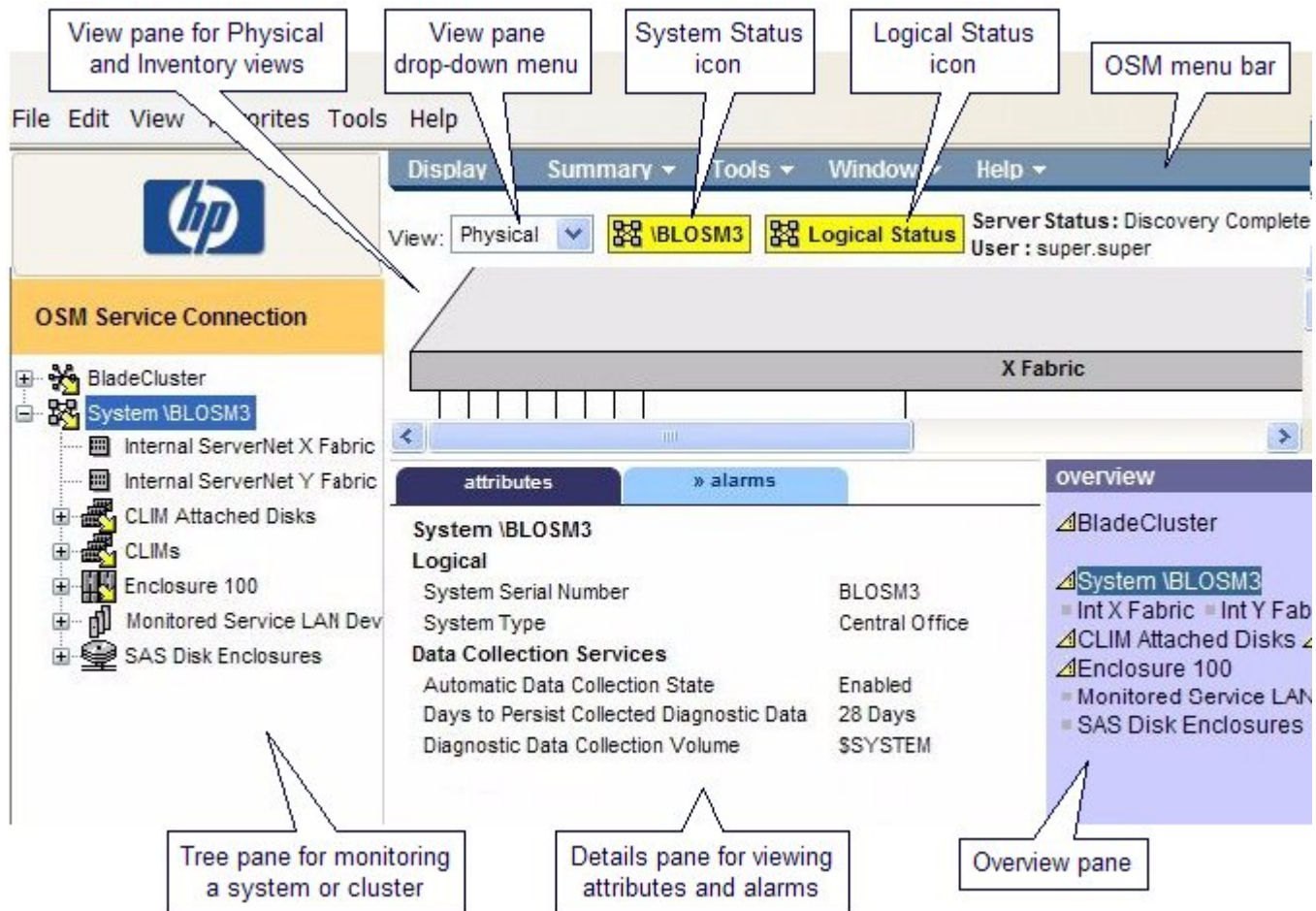
To print management window panes:

1. Select the pane (or browser frame) you want to print.
2. Select **File > Print**.
3. In the Print dialog box, select the location to which you want to print the window and click **Print**.

To save InventoryView information:

1. In the view pane, click **Save**.
2. In the Save dialog box, enter a file name and select the location in which you want to save the pane.
3. Click **Save**.

Management Window Example



Internet Explorer Menu Bar

The Internet Explorer menu bar is not customized for the OSM application. For most OSM functions, use the OSM menu bar (located above the view pane) and the various panes within the Management window. Internet Explorer functions that you might use for OSM include

- Access OSM bookmarks from the Internet Explorer Favorites menu. However, you must use the OSM Create Bookmark function in the Tools menu to create the bookmarks.
- Print the browser frame with focus.
- Use Find to search the contents of the Inventory view.

Internet Explorer features you should **not** use during an OSM Service Connection session:

- The Go To, Stop, or Refresh options from the View menu. For updating OSM attributes and alarms, use the OSM Rediscover action, available by right-clicking on system resource objects.
- You cannot use Internet Explorer's Add to Favorites menu option to create OSM bookmarks. For this functionality, see [Using OSM Bookmarks](#).

OSM Menu Bar Options

The OSM menu bar provides access to OSM-specific functions (in contrast to the [Internet Explorer Menu Bar](#)). With T0682 H02 ABU and later, the OSM menu bar has been redesigned to save space, with just text headings instead of graphic icons. The Logical Status Button has been moved

to a menu option under the [Tools menu](#). This topic describes the options available under each OSM menu.

- △ **CAUTION:** Do not close the Management window when any OSM dialog box is open. You will lose your current service connection.

Display Menu

The Display menu contains the following items:

Attributes	Displays the Attributes dialog box for the selected object. See Using the Attributes Dialog Box to View Attributes .
Actions	Displays the Actions dialog box for the selected object, from which you can perform available actions on selected objects, see the status and progress of ongoing actions, and access action details. See Performing Actions on a Selected Resource .
Alarms	Displays the Alarms dialog box for the selected object. If the selected object has no alarms, this menu item is disabled. See Viewing the Alarms Dialog Box .
Multi-Resource Actions...	Displays the Multi-Resource Actions dialog box, which enables you to perform actions across multiple resources of the same type. See Performing Actions on Multiple Resources of The Same Type .
Resource Views	Displays a list of saved resource configurations. Each configuration represents a view of resources you specified using the Multi-Resource Configuration option on the Multi-Resource Actions dialog box. See Using Resource Views .

Summary Menu

The Summary menu contains the following items:

Problem	Displays the Problem Summary dialog box, which lists all resources that have some type of problem.
Action	Displays the Action Status Summary dialog box, which lists all actions in progress.
Alarm	Displays the Alarm Summary dialog box, which lists the alarms in the current system or ServerNet cluster and enables you to find the resource with the selected alarm in the Management window. If no alarms are outstanding, this menu item is unavailable.
Connection Status	Indicates the current state of all OSM service connection processes. Each IP address listed is associated with a corresponding TCPIP stack configured in the OSMCONF (OSM server configuration) file. You should have at least two connections with a status of UP for fault-tolerance.
System Status	Displays a small dialog box containing a System Status icon , which changes color to indicate problems within the system. This dialog box allows you to monitor several systems while minimizing the Management window for each system to save screen space. (However, closing a Management window also closes the associated System Status window.)

Tools Menu

The Tools menu contains the following items:

Logical Status	<p>Displays the Multi-Resource Action dialog box, pre-configured with a default logical view of your system designed to give you a method for monitoring the health of key system components. This view provides status for all logical processors, disks, LIFs, and SWAN paths.</p> <p>A Logical Status icon is displayed (next to the System Status icon) in the toolbar above the View pane, to indicate at a glance whether or not problem conditions exist on any of the objects included in</p>
-----------------------	---

	<p>the Logical Status view. If the icon turns yellow, select this Logical Status menu option to locate the problem and get details.</p> <p>While the Logical Status view cannot be customized, you can also use the Multi-Resource Action dialog box to create your own resource views; see Using Customized Resource Views.</p>
Event Viewer	Launches the OSM Event Viewer in a separate window. You can also launch the OSM Event Viewer from the Start menu (if you have the OSM client components installed) or directly through an Internet Explorer browser window (without having a current OSM Service Connection session).
Physical Configuration Tool	Launches the Physical Configuration Tool .
Save Snapshot	<p>Displays the Save Snapshot dialog box, which enables you to create and save a snapshot of your system. A snapshot provides information regarding the state of your system and all components at the time that the snapshot file was saved.</p> <p>You can load and view a saved snapshot on any server running OSM server software. To load a snapshot, launch Internet Explorer and enter the URL of the system you are using to view the snapshot, followed by <code>/snapshot/index.html</code>.</p> <p>For example:</p> <p><code>http://star2.caclab.cpqcorp.net:9990/snapshot/index.html</code></p> <p>In the Open Snapshot File dialog box, navigate to and open the snapshot file you want to view.</p>
Reload Configuration Settings	Initiates the process of reloading your OSM server configuration settings. Select Reload Configuration Settings to put into effect any changes made to your OSMCONF file. A dialog will instruct you which OSM processes must be restarted for the reload to be complete.
Create Bookmark	Creates an entry in your Internet Explorer Favorites list for the system you are currently logged on to. Use this bookmark for future access to this system instead of entering the full URL for the system.
Access Control List	Launches the Access Control List dialog box, from which you can manage user access to select OSM actions.

Windows Menu

The Windows menu contains a list of all open OSM windows and dialog boxes in the order they were opened. Selecting a particular menu item brings that window or dialog box to the foreground.

Help Menu

The Help menu contains:

Help Contents	<p>Displays a JavaHelp online help interface to the <i>OSM Service Connection User's Guide</i>. You can also access context-sensitive help topics (from this same JavaHelp interface) directly from the OSM GUI by selecting objects in the GUI and pressing the F1 key, or by clicking Help buttons where provided within GUI dialog boxes.</p>
About OSM	Opens the About dialog box containing OSM product information, such as version number and trademarks.

Rediscover Shortcut Menu Item

Rediscover is supported as an action on all system and some cluster objects. For most objects, Rediscover is available only in the shortcut menu.

Rediscover causes OSM to refresh and reanalyze the object and all subcomponents. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze

refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Using the Physical View

The Physical view is displayed in the view pane of the Management window. You can display the Physical view of either:

- A ServerNet Cluster
- A local system or its components

When you select any resource in the Physical view, its attributes, alarms (if any), and actions are displayed in the details pane.

If the status of a resource is abnormal, a red or yellow triangle appears over it. For more information, see [Interpreting Icons and Color](#). If an alarm is outstanding for the selected resource, a bell icon appears on the Alarms tab in the details pane when you select the resource. For more information, see [Viewing the Alarms Dialog Box](#).

Physical View of the ServerNet Cluster

The Physical View of the ServerNet Cluster displays how your local system is connected to the ServerNet cluster. This view shows the connections between the external X and Y fabrics, your local system, and other remote nodes. The view displays:

- ServerNet cluster X and Y fabrics
- ServerNet cluster switches
- The nodes connected to the cluster switches

To display the Physical view of a ServerNet cluster:

1. In the tree pane, select **ServerNet Cluster**.
2. From the View drop-down list, select **Physical**.

Physical View of a Local System

The Physical view of a local system provides a high-level view of the system configuration and status, showing all groups and external devices such as external disks and SWAN CRUs. The name of the system to which you are connected appears at the top of the view pane.

For more detail on items represented in the Physical view of a system, see the Physical view of an enclosure, the Inventory view, or the details pane.

To display the Physical view of a system:

1. In the tree or Overview pane, select the system name.
2. From the View list, select **Physical**.

Physical View of an Enclosure

The Physical view of a group enclosure is similar to the way the group looks with the enclosure door open. This view shows both the appearance side and the service side of a group. The appearance side is the front view, which you see when you open the door of the enclosure. The service side is the back view. The appearance side appears on the left of the screen, and the service side appears on the right. Inside the group, resources appear inside their slots.

Clicking a resource within the Tree view outlines its location in blue in the Physical view.

Clicking a resource within the enclosure view:

- Outlines it in blue
- Highlights its location in the Tree view
- Displays its attributes in the Detail view

To display the Physical view of an enclosure:

1. In the tree or Overview pane, click a group.
2. From the View list, select **Physical**.

Physical View of a Fabric

The Physical view of a fabric provides an overview of the internal ServerNet X and Y fabrics and the processors and groups connected to them. You can also view a single fabric and the processor switches and IOAM enclosure connected to it.

Clicking a resource within the Tree view outlines its location in blue in the Physical view.

Clicking a resource within the fabric view:

- Outlines it in blue
- Highlights its location in the Tree view
- Displays its attributes in the Detail view

To display the Physical view of a fabric:

1. In the tree or Overview pane, click a fabric or processor group.
2. From the View list, select **Physical**.

Using the Inventory View

The Inventory view contains a list of resources and select attributes. It is located in the view pane of the Management window. You can display an Inventory view of a ServerNet Cluster or a local system.

You can select a resource in the Inventory view and display its attributes or alarms (if any) or perform actions on it. If an alarm is outstanding for the selected resource, a bell icon appears on the Alarms tab in the details pane when you select the resource. For more information, see [Viewing the Alarms Dialog Box](#).

To find a resource in this view, use the browser's Find function. For more information, see [Using the Browser's Find Feature](#).

To display the Inventory view:

1. From the tree or overview pane, click **ServerNet Cluster** or **System**.
2. From the View list, select **Inventory**.

Inventory View of a ServerNet Cluster

The Inventory view of a ServerNet Cluster displays a complete or partial list of resources in the cluster, depending on the resource you select in the tree pane.

The Inventory view of a ServerNet cluster displays:

Name	The logical name of a component in the cluster and the switch zone and fabric in which it is located. For example: Switch Group 1020 (the switch group in zone 2 on the X fabric)
Serial Number	A unique identification number assigned to a external switch port.
Type	The type of switch plug-in card (such as Router Interconnect) or transceiver (such as 9/125 Micron SMF).
Power State	Indication of whether the component is powered on or off.
Hardware Revision	The hardware design revision, similar to a version number.

Track ID	The unique number assigned to every component. If you know a component's part number and tracking ID, you can find its exact location in the system.
Part Number	The part number assigned to the component. Use this part number to order a replacement component.

Inventory View of a Local System

The Inventory view of a local system displays a complete or partial list of resources in it, depending on the system resource you select in the tree pane.

If you select	The Inventory view displays
The system	The system and all of its resources.
An individual resource	The selected resource and other resources in the corresponding group. Components that contain the resource, such as the system, do not appear.
An external disk	All external disks in the server.

Each row lists one component, with adjacent columns listing the following information about each component:

Name	The logical name of a component in the system and the slot in which it is located. For instance, DISK \$DATA (1.2.7) is the name of a disk in Group 1, Module 2, Slot 7.
Serial Number	A unique identification number assigned to a component when it is manufactured.
Type	Indication of the type of plug-in card, such as ECL or SSAC.
Power State	Indication of whether the component is powered on or off.
Hardware Revision	The hardware design revision, similar to a version number.
Track ID	The unique number assigned to every component. If you know a component's part number and tracking ID, you can find its exact location in the system.
Part Number	The part number assigned to the component. Use this part number to order a replacement component.

Using Shortcut Menus

The shortcut menu is available for all selectable system and cluster resources. These resources include the overview pane, tree pane, and the Physical and Inventory views in the View pane, as well as dialog boxes with selectable resources. To display a shortcut menu, right-click a resource.

The shortcut menu for all resources contains these choices:

Attributes	brings up the Attributes dialog box for that resource.
Alarms	brings up the Alarms dialog box for that resource. The Alarm menu item is unavailable if there are no alarms on the resource.
Actions	brings up the Action dialog box for that resource.

All system resources also contain this choice:

Rediscover	causes OSM to refresh and reanalyze the object and all subcomponents. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.
-------------------	---



















The only cluster resources that have the Rediscover action are the ServerNet Cluster and External ServerNet Fabric.

Interpreting Icons and Color

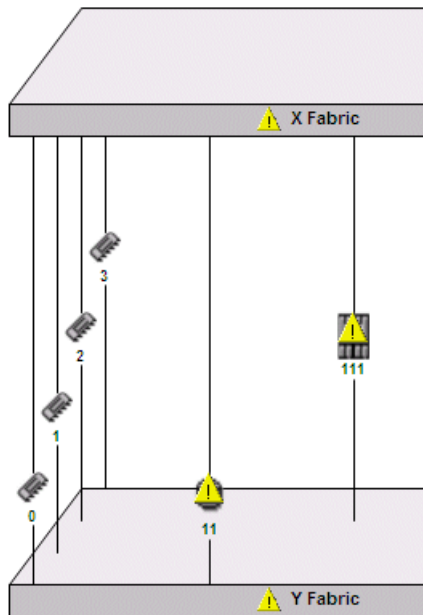
The OSM Service Connection uses different icons and colors to indicate a change from normal status in a group or resource in the Management window.

The states are indicated as green (normal), yellow (warning), and red (critical). See [Alarm Severity](#).

State Indicators

<p>The color of System Status icon (the left icon in each example) and Logical Status icon (the right icon in each example) in the view pane indicates the overall state of the system and Logical Status objects.</p> <p>While you can suppress alarms and problem attributes to acknowledge problems on the System Status icon (thus keeping the icon green unless other problems occur that you have not suppressed), suppression has no effect on the Logical Status icon. It remains yellow even if problem conditions within those components are suppressed.</p>	<div> \OSM3  Logical Status</div> <p>Green icons indicate that no problems exist within the system or the Logical Status components (the System Status icon can also be green if all problem conditions are suppressed).</p> <div> \OSM3  Logical Status</div> <p>A yellow System Status icon indicates that problem conditions exist somewhere within the system (although, in this example, not within the objects represented by the Logical Status icon).</p> <p>To locate the source of any problems, expand the System or ServerNet Cluster object in the tree pane (whichever is displaying a yellow arrow over its icon) and drill down (expanding icons displaying yellow arrows) until you locate the component displaying an alarm or problem attribute.</p> <p>If the Logical Status icon is yellow, select Logical Status from the Tools menu on the OSM menu bar to learn which of those components is reporting a problem.</p>
<p>A red or yellow icon displayed over a resource indicates that it requires service or operational intervention.</p>	<div> Battery (1.1.23)</div> <div> Disk \$DSMSCM-P (11.1.15)</div>
<p>Icons in the overview pane show the state of various resources.</p>	<div>overview</div> <div> System \OSMDRP</div> <div> Group 11  Group 111</div> <div> Group 400</div> <div> Fabric Group 100</div>
<p>In the tree pane, a yellow icon displayed over a system, group, module, or any parent object that contains subcomponents indicates that one or more subcomponents require service or operational intervention.</p>	<div> Fabric Group 100</div> <div> Internal ServerNet X Fabric</div> <div> Internal ServerNet Y Fabric</div> <div> Processor Switch 100.3</div> <div> Maintenance PIC (100.3.1)</div> <div> (100.3.2)</div> <div> ServerNet PIC (100.3.3)</div>

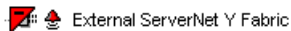
State icons are also shown in the Physical view of a cluster or system.



Alarm Indicators

If the object has at least one alarm, an alarm icon appears:

In the tree pane



On the alarms tab and detail



In the Alarm Summary

Severity +	Creation Time	IndicationIdentifier	Description
Critical	Jan 18, 2005 09:17:23 AM PST	(100.2.2)	Unknown CRU
Critical	Jan 18, 2005 09:17:23 AM PST	Power Supply (100.2.18)	Hardware Error
Major	Jan 18, 2005 09:17:28 AM PST	IOAM Enclosure 111	Midplane FIR Mismatch
Major	Jan 18, 2005 09:17:23 AM PST	Power Supply (100.2.18)	AC Power Loss

Alarm Severity

Critical	Immediate corrective action is required. A service-affecting fault occurred. For example, a resource might have become unavailable.
Major	Urgent corrective action is required. A service-affecting fault has developed. For example, a resource might have lost fault tolerance.
Minor	A fault exists that does not affect service. Corrective action should be taken to prevent a more serious fault. For example, an unexpected path change occurred.

Warning	A potential or impending service-affecting fault was detected before any significant effects are evident. For example, retrievable errors exceeded a threshold.
Cleared	This alarm is no longer in effect. Typically, alarms are cleared because the affected resource has been repaired or the fault condition no longer exists.
Indeterminate	The severity level cannot be determined.

Using the Browser's Find Feature

You can use your browser's Find feature to search the local system or ServerNet cluster for a resource. This feature is especially useful on large systems or clusters.

To find a resource:

1. In the tree pane, select **System** or **ServerNet Cluster**, depending on the type of resource you want to find.
2. From the view pane drop-down list, select Inventory. If the Inventory view is already displayed, click one of its column headings to ensure that the view pane is active.
3. From the browser's Edit menu, select **Find [on This Page]...**
4. Type a resource name or an attribute value associated with the resource you want to find.
5. Click **Find Next**. If a resource with a matching value is found, the matching text is selected in the Inventory view.
6. Click the matching text to select the resource. Information about the resource appears in the details pane.

If no resources contain the specified value, a message informs you that the search text was not found.

To search for the next occurrence of the specified value, click **Find Next**.

Examples

To search for a specific disk drive, enter all or part of its name, such as \$DATA2, in the find text box.

- To search for a particular type of disk drive, enter its part number, such as 425752, in the find text box.
- To search for any MSEB, enter MSEB in the find text box.

6 Viewing Alarms

When certain problem conditions exist on a system, OSM generates alarms on the objects in need of service or attention.

Alarms can be viewed in these ways:

- Alarms associated with a specific resource:
 - Right-click the object and select **Alarms** to display the [Alarms dialog box](#).
 - Click the [Alarms Tab](#) of the Details pane to view alarms for the selected object.
- A summary of alarms for the entire server or ServerNet cluster; see [Viewing a Summary of Alarms](#).

To view more details, including suggested repair actions, and to save alarm details, see [Viewing Alarm Details](#).

To act on individual alarms, see:

- [Deleting Alarms](#)
- [Suppressing Alarms](#).

Viewing the Alarms Tab

The details pane displays attribute and alarm information about a selected resource, depending on which tab you select. If there are any alarms for a selected resource, a bell icon appears on the Alarms tab.

The Alarms tab provides this information about the selected alarm:

- Alarm severity

The Severity column contains a colored icon corresponding to the severity of the alarm. Red icons represent Critical and Major alarms. Yellow icons represent Minor, Warning, and Indeterminate alarms. See [Alarm Severity](#).
- Time and date the alarm occurred
- Description of the alarm, including the probable cause
- Whether the alarm is dialed out to your service provider (assuming your system console is configured to dial out).

To view alarms in the Alarms tab:

1. In either the tree or view pane, click a resource.
2. In the details pane, click the Alarms tab to display the alarms for the selected resource.

For additional alarm details, right-click on the alarm and select **Details**.

To act on alarms in the Alarms tab:

Right-click on the alarm and select:

- [Delete](#)
- [Suppress](#)
- [Unsuppress](#)

Viewing the Alarms Dialog Box

To reach this dialog box, either:

- Right-click any object in the tree pane or view panes and select Alarms.
- Highlight any object in the tree pane or view panes and select Alarms from the Display menu.

The Alarms dialog box displays the alarms associated with a selected resource. You can select individual alarms for the resource and display detailed information and available repair actions or act on those alarms. To view a summary of alarms for the entire system, see [Viewing a Summary of Alarms](#).

The Alarms dialog box provides this information about the selected alarm:

- Alarm severity
The Severity column contains a colored icon corresponding to the severity of the alarm. Red icons represent Critical and Major alarms. Yellow icons represent Minor, Warning, and Indeterminate alarms. See [Alarm Severity](#).
- Time and date the alarm occurred
- Description of the alarm, including the probable cause
- The type of alarm
- Whether or not the alarm is suppressed
- Whether the alarm is dialed out to your service provider (assuming your system console is configured to dial out)

The **Save** button in the Alarms dialog box allows you to save an html file containing detailed alarm information. This file contains detailed information for every alarm currently existing on the system, not just those on the selected object or alarm.

You can also view alarms for a selected resource without opening the Alarms dialog box as explained in [Viewing the Alarms Tab](#).

To display detailed information for an alarm:

Highlight the alarm and then click **Detail**. See also [Viewing Alarm Details](#).

To act on an alarm:

Highlight the alarm and click:

- [Delete](#)
- [Suppress](#)
- [Unsuppress](#)

Viewing Alarm Details

The Alarm Detail dialog box provides this information about the selected alarm:

- Name of the resource associated with the alarm
- Whether the alarm is dialed out to your service provider (assuming your system console is configured to dial out)
- Time and date the alarm occurred
- Alarm type and severity
- Probable cause and description of the alarm
- Repair actions

To save alarm detail and repair information:

Click **Save**. In the Save As dialog box, specify a file name and folder and click **Save**. The information is saved as a text file.

To reach this dialog box:

In the Alarm dialog box or Alarm Summary dialog box, select an alarm and click **Detail**.

Suppressing Alarms

To stop known problems from propagating up and causing higher level object icons to indicate problem conditions within, you can choose to suppress a particular alarm type on a specific system resource.

To suppress an alarm:

Select, then right-click an alarm in the Alarms tab, Alarms dialog box, or the Alarm Summary dialog box and click either **Permanent** or **Temporary** suppression, as desired:

- If you select **Permanent** suppression and the same alarm is generated again on this object at a later time, state propagation will not occur.
- If you select **Temporary** suppression and the same alarm is generated again on this object at a later time, state propagation will occur.

To undo the alarm suppression, select the alarm, right-click and choose **Unsuppress**.

Suppression Persistence

With OSM T0682 H02 ABX and later, suppression of state propagation resulting from alarms and problem attributes is set, by default, to persistent. That is, the suppression that was specified in the OSM Service Connection will remain in effect even after cold loads or restarting the OSM server. To disable this persistence and make all suppression valid only for the current OSM server session, see the *OSM Configuration Guide* for the necessary OSMCONF parameters.

Deleting Alarms

To delete an alarm, right-click the alarm in either the Alarms tab, Alarms dialog box, or the Alarm Summary dialog box and select Delete. (In the Alarms dialog box or the Alarm Summary dialog box, you can also highlight the alarm and click the Delete button.)

7 Viewing Attributes

Every resource has attributes associated with it. You can view the attributes of a resource in the details pane of the Management window, or you can display the Attributes dialog box, which is available from any view.

To view attributes for a selected resource without opening the Attributes dialog box, see [Using the Details Pane to View Attributes](#).

For further information on viewing the Attributes dialog box, see [Using the Attributes Dialog Box to View Attributes](#).

Using the Details Pane to View Attributes

The details pane displays information about a selected resource. The type of information displayed depends on which tab is selected in the details pane:

1. In either the tree pane or the view pane, select a resource.
2. In the details pane, click the Attributes tab to display the attributes for the selected resource.

Using the Attributes Dialog Box to View Attributes

The Attributes dialog box displays the attributes associated with a selected resource and allows you to display the actions that you can perform.

Any problematic attribute that might require attention is preceded by a colored icon. Yellow indicates a warning, and red indicates a critical state.



To show actions for a resource:

Click **Show Actions** to display the Actions dialog box for the resource.

To save the list of attributes:

Click **Save** to display a Save dialog box.

To reach the attributes dialog box:

Do one of:

- In the tree view, select a resource and select **Display > Attributes**.
- Right-click any resource and select **Attributes** from the menu that appears.
- In the physical view, right-click a resource and select **Attributes** from the menu that appears.

Suppressing Problem Attributes

To stop known problems from propagating up and causing higher level object icons to indicate problem conditions within, you can choose to suppress a particular problem attribute value on a specific system resource. Problem attributes are those displaying yellow or red flags next to the attribute name.

To suppress a problem attribute:

Select, then right-click a problem attribute in either the Attributes tab or Attributes dialog box and click either **Permanent** or **Temporary** suppression, as desired:.

- If you select **Permanent** suppression and the same attribute value is generated again on this object at a later time, state propagation will not occur.
- If you select **Temporary** suppression and the same attribute value is generated again on this object at a later time, state propagation will occur.

To undo the attribute suppression, select the attribute, right-click and choose **Unsuppress**.

While you cannot suppress a Service State attribute value, you can suppress the alarm that is causing the Service State attribute value to be degraded. See [Suppressing Alarms](#). Once the alarm is suppressed, the Service State attribute value changes to Problem Acknowledged.

Suppression Persistence

With OSM T0682 H02 ABX and later, suppression of state propagation resulting from alarms and problem attributes is set, by default, to persistent. That is, the suppression that was specified in the OSM Service Connection will remain in effect even after cold loads or restarting the OSM server. To disable this persistence and make all suppression valid only for the current OSM server session, see the *OSM Configuration Guide* for the necessary OSMCONF parameters.

8 Performing Actions

You can perform and monitor actions as follows:

- Perform a specific action on a selected resource: [Performing Actions on a Selected Resource](#).
- Perform a specific action on several resources of the same type: [Performing Actions on Multiple Resources of the Same Type](#).
- Perform a firmware update on a specific resource: [Performing Firmware Updates](#).
- View a summary of actions in progress and recently completed: [Viewing a Summary of Actions](#).
- View detailed information about an actions in progress or recently completed: [Viewing Action Details](#).
- [Abort an Action](#) (where applicable).

NOTE: Some actions require super-group access. If you are not logged on as a super-group user and attempt to initiate an action that requires super-group access, a message advises that you are not authorized to perform the action.

Some key actions must (or can) be performed in the OSM Low-Level Link application. For more information, see [Related System and Processor-Level Recovery Actions](#) or the OSM Low-Level Link online help.

Controlling Access to Actions

With OSM version T0682 H02 ACJ and later, the Access Control List feature within the OSM Service Connection provides greater flexibility for controlling access to specific OSM actions. Previously, there were two levels of control that could not be configured: one set of actions that could be performed by super group users only and the rest of the actions, which could be performed by all non-super group users as well. This new Access Control List feature is applicable only to actions tied to OSM infrastructure commands and **not** those executed via the SPI and Guardian interface, so as to not conflict with the command authorization settings already in place for SPI subsystems.

Changes made to access control settings are system-wide, not console-specific. In other words, any changes made apply to that NonStop system regardless of where a user logs on from. You can leverage access control settings by migrating the settings created on one NonStop system to other NonStop systems (see [Migrating Access Control List Settings](#)).

To launch the Access Control List dialog box, select **Access Control List** from the [Tools menu](#) on the OSM menu bar. In the example below, the box under the Roles heading lists the three default roles that OSM provides for each system; any additional roles that you create are displayed here also. When you select a role, you can see the members assigned to that role, the privileges granted to all members – that is – the names of the OSM actions that can be performed by the members of that role, as well as a comments field for an optional description of the role.

BLOSM3 - Access Control List

Roles

Everyone
NonStop Super Group Users
NonStop Super ID

Add Role
Restore Default Roles

Description

Role Name: Everyone

Comments:

Members: *, *

Add Member
Delete Member

Privileges:

- ☐ Collect Diagnostic Data
- ☐ Delete Alarm
- ☐ Enable/Disable Automation of Data Collection
- ☐ Extend Problem Incident Report Suppression Time
- ☐ Manage Access Control List
- ☐ Set Data Collection Volume
- ☐ Set Days to persist for Diagnostic Data
- ☐ Suppress Alarm State Propagation
- ☐ Suppress Attribute State Propagation
- ☐ Suppress Problem Incident Report Creation
- ☐ Test Incident Report Delivery Paths
- ☐ Unsuppress Alarm State Propagation
- ☐ Unsuppress Attribute State Propagation
- ☐ Unsuppress Problem Incident Report Creation

Add All Privileges
Remove All Privileges

Save Role
Delete Role

Create Report
Close
Help

Behavior for the three **Default Roles** is as follows:

- **NonStop Super ID** – No changes can be made to this default role, in terms of membership or privileges, nor can this role be deleted.
- For the default roles **Everyone** and **NonStop Super Group Users**, cannot add or delete members, but you can change the privileges assigned to those roles. You can delete a selected role using the **Delete Role** button or restore them if they have been deleted by using the **Restore Default Roles** button.

NOTE: The **Restore Default Roles** button restores either of these two default roles if they have been deleted. It does not restore the privilege settings for *existing* default roles. If you want to restore the default privilege settings for a default role, you could accomplish that by first deleting the role, then using the **Restore Default Roles** action to restore the role – when a deleted default role is restored, the privilege settings will revert to default values.

You can create a new role by clicking **Add Role**. When you do so, you are prompted to specify a role name and can optionally add comments that are displayed whenever that role is selected

in this dialog box. You can add members to the new role by clicking **Add Member**. Under Privileges, select the actions that can be performed by the members of this role. Any OSM actions not listed here are actions that cannot be restricted through the Access Control List functionality. Click **Save Role** to save the role and have it added to the list of available roles. You can delete members from a role by using the **Delete Member** button or delete a selected role by clicking **Delete Role**.

You can click **Create Report** to create and save a report showing the details for each role on the system. These reports are saved, in .csv format (best opened through Microsoft Excel or WordPad), to the console from which it is created. The default location is: Documents and Settings\user-name\Application Data\HP\OSM.

The access control feature is enabled by default in T0682 H02 ACJ and later, but can be disabled through a setting in your OSMCONF file. For information on disabling the feature, see the *OSM Configuration Guide*

Migrating Access Control List Settings

If you create or customize roles for one NonStop system, you can use the following procedure to migrate those settings to other NonStop systems:

1. On the system from which you want to migrate the settings, copying the ACLREPO file located in \$system.zservice.
2. On the system to which you want to migrate the settings, stop the CIMOM process, then copy the ACLREPO file from the other system to \$system.zservice (overwriting the existing file, if one exists).
3. If the system you are migrating to has an existing ACLREBAK in \$system.zservice (this is a backup file for ACLREPO), purge the existing file before restarting CIMOM.
4. Restart the CIMOM process. The system will inherit the access control settings from the system that the ACLREPO file was copied from, and a ACLREBAK backup file will be created automatically.

Performing Actions on a Selected Resource

Use the Actions dialog box to perform actions on a selected resource in the server or ServerNet cluster. Actions for the selected resource appear in the Available Actions list.

For a description of a particular action, highlight the action and press the F1 key.

A history of actions performed on the resources within the last eight hours appears in the Action Status list. (Eight hours is the default, which is configurable.)

To reach the Actions dialog box:

1. Right-click a resource.
2. From the menu that appears, select **Actions**.

Performing an Action

1. From the Available Actions menu, select the action to be performed.
2. Click **Perform action**:
 - a. If the action requires you to set a parameter, a parameter box appears. Enter the appropriate parameter value and click **OK**.
 - b. Some actions require you to respond to a confirmation message before the action is performed.
3. In the Action Status box, monitor the status of the action being performed.

Viewing Detailed Information About an Action

1. In the Action Status list, select the action whose details you want to view.
2. Click **Details** to display the Action Detail dialog box.

The Action Detail dialog box provides a description of the action, the resource acted on, and the action status. The detail also includes the cause, effect, and repair action for any failed action.

Aborting an Action

In the Actions dialog box, click the **Abort action** button, if available, to stop an OSM action in progress (it is not available if the button is "grayed out").

Performing Actions on Multiple Resources of the Same Type

Use the Multi-Resource Actions dialog box to perform an action on a group of resources of the same type. The dialog box allows you to select the resource type. All resources of that type appear in an available resources list, and actions for the selected resource type appear in the Action drop-down menu. You can select an action and then select specific resources on which to perform the action. Based on the selected action, you can also specify a filter category to further refine the resource list.

The Multi-Resource Actions dialog box has been enhanced with a new look and to provide customizable [Resource Views](#) and a default [Logical Status](#) view of your Integrity NonStop NS-series servers.

To reach the Multi-Resource Actions dialog box:

Do one of:

- Select **Display > Multi-Resource Actions**.
- In the Action dialog box, click **Multi-Resources**.

Performing an Action

1. From the Resource Type drop-down list, select the type of resource on which to perform the action. (If you reach this dialog box from the Actions dialog box, the resource selected in the Actions dialog box appears in the Resource Type box.)

All resources of the selected type appear in the available resources list.

2. From the Action drop-down menu, select the action to perform. A second resources list is displayed below the first.
 - a. You can resize the panes by using the divider line above the add and remove buttons.
 - b. You can sort either resources list by clicking the bottom line of the column heading.
3. To further refine the resources on which to perform the action, select a parameter from the Filter by drop-down menu. Only resources in the available resources list with the specified characteristic are displayed.

Some actions, such as SP Firmware Updates should not be performed on all SPs simultaneously. For these potentially disruptive actions, the Filter by menu forces you to choose between X-fabric or Y-fabric SPs.

4. Select the specific resources on which to perform the action:

Select	To
Add all	Move all resources in the available resources list to the selected resources list. (The Add all button is enabled only when no resource in the available resource list is highlighted.)
Add	Move a specific resource (selected by clicking it) from the available list to the selected list.
Remove all	Move all resources from the selected list back to the available list.
Remove	Move a specific resource (selected by clicking it) from the selected list back to the available list.

5. Click **Perform Action**.

As the action is performed, its status appears to the left of the resource name in the selected resources list.

A summary of the action progress is shown in the Progress status boxes.

6. To view a summary of the actions, click **Action Summary**. (For information on action details, see [Viewing Action Details](#).)

Saving a Multi-Resource View

You can now save information (in Microsoft Excel format) displayed in the Multi-Resource Actions dialog box, either for the selected resource or for all resources, by clicking the **Save** button.

Using Customized Resource Views

Creating and Saving a Customized Resource View

You can create and save your own customized resource view -- a view that only includes those objects that you have selected. Then, in the future, you can select this resource view from Display > Resource Views:

1. In the Multi-Resource Actions dialog box, click **Configure....**
2. In the Multi-Resource Configuration dialog box, enter a name for your customized resource view.
3. Use the check boxes next to the resources to select those you want saved in your view. **Select All** and **Deselect All** help refine the list resources.
4. You can further refine the resource view by selecting which attribute groups to save, such as Logical or Firmware. Expand a resource and use the check boxes to select attribute groups.
5. Click **Save** to save your customized resource view for future use.

Selecting a Saved Resource View

1. From the Display menu on the OSM menu bar, select Resource Views and then the name of the previously saved resource view you want to view. (Within the Multi-Resource Actions dialog box, you can also select a previously saved resource view from the Configuration list.)
2. The Multi-Resource Actions dialog box is displayed. Only the resources specified in the saved resource view appear under Resource Types.

Deleting a Resource View

1. In the Multi-Resource Actions dialog box, click **Configure....**
2. In the Multi-Resource Configuration dialog box, select the name of the resource view you want to delete from the drop-down menu.
3. Click **Delete**.

Viewing Action Details

The Action Detail box provides a description of a selected action, the resource acted upon, and the action status. The detail also includes the cause, effect, and repair action for any failed action.

To reach this dialog box:

Do one of:

- In the Action Status list of Action dialog box, select the desired action and click **Details**.
- In the Action Status list of Multi-Resources Action dialog box, select the desired action and click **Details**.
- In the Action Status list of the Action Status Summary dialog box, select the desired action and click **Details**.

Performing Firmware Updates

To update down-rev firmware for a specific resource, use one of the actions available for that resource.

NOTE: NonStop NS-series processor firmware is updated through a guided procedure rather than the Multi-Resource Actions dialog box. Launch the guided procedure by performing the Firmware Update action on the individual Processor Complex object. (This action cannot be performed from the Multi-Resource Actions dialog box.) Follow the procedure and online help.

Performing a Firmware Update

1. Select **Display > Multi-Resource Actions**.
2. From the Resource Type drop-down list, select the type of resource on which to perform the firmware update. All resources of the selected type appear in the available resources list.
3. From the Action drop-down menu, select the action to perform. A second resources list is displayed below the first:
 - You can resize the panes by using the divider line above the add and remove buttons.
 - You can sort either resources list by clicking the bottom line of the column heading.
4. To further refine the resources on which to perform the firmware update, select a parameter from the Filter by drop-down list. Only resources in the available resources list with the specified characteristic are displayed.

Some actions, such as SP Firmware Updates should not be performed on all SPs simultaneously. For these potentially disruptive actions, the Filter by menu forces you to choose between X-fabric or Y-fabric SPs.

The Compare State - Down-rev parameter is shown only if any down-rev firmware actually exists.

5. Select the specific resources on which to perform the action:

Select	To
Add all	Move all resources in the available resources list to the selected resources list. (The Add all button is enabled only when no resource in the available resource list is highlighted.)
Add	Move a specific resource (selected by clicking it) from the available list to the selected list.
Remove all	Move all resources from the selected list back to the available list.
Remove	Move a specific resource (selected by clicking it) from the selected list back to the available list.

6. Click **Perform Action**.

As the firmware update is performed, its status appears to the left of the resource name in the selected resources list.

A summary of the action progress is shown in the Progress status boxes.

7. To view a summary of the actions, click **Action Summary**. (For information on action details, see [Viewing Action Details](#).)

Launching Guided Procedures

For a list of available guided procedures, see [OSM Guided Procedures](#).

Using the Physical Configuration Tool

Modular systems can exist in physical configurations spread over several different racks. With T0682H02 AAN and later, the OSM Service Connection provides a Physical Configuration Tool that you can use to create and save a physical display of the racks in which your modular system resides.

With T0682H02 ADL and later, the **Add Rack** action in the Physical Configuration Tool allows you to add an optional Rack Location value to help differentiate between the various racks displayed in the Physical Configuration Tool. While up to 80 characters can be specified, the name will be truncated to 30 characters in the Physical Configuration Tool window. To assign a Rack Location value to a rack already displayed in the Physical Configuration Tool without such a value, use the "Locator" parameter in the **Set Physical Location** action on one of the objects within that rack. Then, upon restarting the OSM Service Connection session, that "Locator" value will be displayed as the Rack Location for that rack within the Physical Configuration Tool.

To launch the tool, select Physical Configuration Tool from the [Tools menu](#) of the OSM Service Connection. Upon launching, the Physical Configuration Tool displays whatever OSM knows about the current physical configuration of your system. This information is based solely on Rack Name and Rack Offset values assigned by OSM users through individual Set Physical Location actions on modular components. This action is available (depending on system type) for [Blade Elements](#), [BladeSystem Enclosures](#), [FCDMs](#), [IOAM Enclosures](#), [Processor Switch Modules](#), [Processor Components](#), and [VIO Modules](#). The problems with this information include:

- Components not assigned Rack Name and Rack Offset values are displayed in the Unconfigured FRUs pane rather than in the Configured Racks pane.
- Components given even slightly overlapping Rack Offset values are displayed in the Incorrectly Configured FRUs pane. Their locations in the Configured Racks pane are displayed as yellow, unlabeled areas.
- If you moved a component but did not use the action to update it, it continues to be displayed in the old (incorrect) location.
- If Rack Names are not precise (for example, if one FCDM is designated as Rack 1, another in the same rack is designated as rack 01), the Physical Configuration Tool displays those as two separate racks.

Now you do not need to use the Set Physical Location* action to specify Rack Name or Rack Offset. Instead, you can use the Physical Configuration Tool to:

- Drag and drop components between and within the panes to accurately depict your actual physical configuration.
- Click Add Rack to add new racks to the Configured Racks pane.
- Save the physical view to an HTML file for use outside of OSM.

* The Set Physical Location action still has value, in case you want to assign an additional (optional) Locator text string or Alarm Panel Identifier (used for Telco systems only).

[Monitored Service LAN Devices](#) objects do not have a Set Physical Location action; however, the Rack Name and Offset values can be set by placement of the objects through the Physical Configuration Tool.

For illustrated information on using the Physical Configuration Tool, see the *OSM Configuration Guide*.

9 Viewing Summary Reports

You can view a:

- [Problem Summary](#)
- [Summary of Actions](#)
- [Summary of Alarms](#)
- [Resource Summary](#)

Viewing a Problem Summary

The Problem Summary lists all resources that are in a problem state. The report lists this information:

- The name of the problem resource
- The Service State (See possible [values](#).)
- The attribute group in which the problem occurs
- The attributes in which the problem occurs

To create the report:

Select **Summary > Problem**.

Viewing a Summary of Actions

The Action Status Summary displays a summary of all actions in progress and actions that have taken place in past 24 hours. Information for each action includes resource name, action name, action status, and progress of the action. You can also view detailed information about each action.

Actions Not Displayed

The Rediscover action is not reported in the Action Summary dialog box. (This action updates the OSM client interface and is not really an action performed on the system resources themselves.)

OSM Software-Triggered Actions

The Action Summary dialog box also displays actions initiated automatically by OSM software. An **Internal Refresh** action on a processor is triggered and reported as a result of these activities:

- A Rediscover action on a module
- Firmware Update actions
- SP state changes

Viewing Action Details

1. In the Action Status list, select the action for which to view details.
2. Click **Detail**. The Action Details dialog box appears and provides detailed information about the action.

To reach this dialog box:

Select **Summary > Action**.

Viewing a Summary of Alarms

The Alarm Summary displays a list of alarms in the server or ServerNet cluster. The dialog box allows you select individual alarms for the resource and display detailed information and repair actions that you can perform to correct them. You can use the Alarms dialog box to view the alarms for a single resource, as described in [Viewing the Alarms Dialog Box](#).

The Alarm Summary dialog box provides this information about each alarm:

- Alarm severity
- Time and date the alarm occurred
- Resource name
- Description of the alarm, including probable cause and alarm type
- Whether or not the alarm is suppressed
- Whether the alarm is dialed out to your service provider (assuming your system console is configured to dial out)

To display detailed information for an alarm:

Highlight the alarm and click **Detail**. Or right-click the alarm and select **Detail** from the menu that appears. See [Viewing Alarm Details](#).

To suppress or unsuppress an alarm: see [Suppressing Alarms](#).

You can suppress the state propagation that results when a specific alarm type occurs on a selected object. By suppressing the alarm, state propagation will not occur if the same alarm is again generated on the object. Unsuppressing an alarm resumes the state propagation.

To delete an alarm:

Highlight the alarm and click **Delete**. Or right-click the alarm and select **Delete** from the menu that appears.

To sort the alarms:

When you first open the Alarm Summary dialog box, the alarms are sorted in chronological order. To sort the alarms in a different order, click a column header. An icon next to the column heading indicates which field controls the sort order. 

To save alarm information:

The **Save** button in the Alarm Summary dialog box allows you to save an html file containing detailed alarm information. This file contains the details for every alarm currently existing on the system, not just those on the selected object.

To reach this dialog box:

Select **Summary > Alarm**.

Viewing a Resource Summary

Use the Multi-Resource Actions dialog box to build a summary of any collection of resources of the same type:

1. Select **Display > Multi-Resource Actions**.
2. From the Resource Type list, select a resource to display all resources of that type.
3. To perform an action on any of the resources, see [Performing Actions on Multiple Resources of the Same Type](#).

10 Managing a System

A system consists of all the hardware components, software, and firmware that are managed by a single operating system.

Using the OSM applications, you can monitor and maintain your local server to check the status of all system components and to watch for indications of potential system problems. You can also [perform OSM actions](#) to resolve many system problems. For details about the resources that make up a system, see [System Resources](#).

Locating and Viewing System Resources

1. Expand the system resource in the tree pane to see its resources.
2. In the View drop-down menu, you can select different views of the system:
 - The Physical view depicts the resources within the system.
 - The Inventory view lists the resources within the system in tabular format.

Monitoring a System

System monitoring tasks include:

- Viewing alarms for resources in the system. Look for alarm bell icons and red and yellow triangle icons. These icons appear in the Management window and Alarm dialog box identifying which resources need operator attention or some other type of service. See [Viewing a Summary of Alarms](#).
- Viewing the attributes of a selected resource in the system. If you suspect that a resource is having problems, you can check the attributes of the resource in the Attributes dialog box. Attributes identify information such as the name of the resource, type of resource, and state of the resource. See [Viewing Attributes](#).
- Checking the [OSM Event Viewer](#) for events. The OSM Event Viewer displays events from EMS-formatted log files such as \$0 and \$ZLOG.
- Checking the internal X and Y fabrics to examine the system's connections between its groups. Use the [Group Connectivity ServerNet Path Test](#) action for the Internal ServerNet Fabric resource.
- Checking for status messages or error messages that occur during your OSM service connection. These messages are logged in the Microsoft Windows Event Viewer Log.

Performing Actions on a System

With System selected in the tree pane drop-down list, you can access and perform actions on resources within a system. To perform an action on a system, select System in the tree pane and then navigate to the system resource on which you want to perform an action. See [Performing Actions](#).

Updating Firmware

You can update firmware for many resources, including the service processor, selected resources, and the cluster switch. See [Performing Firmware Updates](#).

11 System Resources

Using OSM, you can monitor and maintain these system resources:

Alarm Panel	FESA	Processor Blade
4PSE	Fiber (Blade Switch Port)	Processor Components
ATM Adapter	Fibre Channel Router	Processor Switch Module
ATM Line	FSAC	SAC
Battery	G4SA	SAS Card (CLIM)
Blade Complex	G4SA PIF	SAS Disk Enclosure
Blade Element	G4SA SAC	SAS Disk Enclosures
Blade Element Firmware	GESA	SCSI Controller
Blade System Board	Group (IOAM, Fabric, or G16SE)	ServerNet Interface Card (Blade)
Blower (FCDM)	Group (IOMF2 or VIO)	ServerNet Interface Card (CLIM)
CCSA	Hard Disk (CLIM)	ServerNet PIC
CLIM	InfiniBand HCA Card (CLIM)	ServerNet Port
CLIMs	Internal ServerNet Fabric	ServerNet Switch (Blade Enclosure)
CLIM-Attached Disks	IO Module (SAS Disk Enclosure)	ServerNet Switch Board
DIMM (CLIM)	IOAM	Service Processor
Disk	IOAM Enclosure	Smart Array Controller (CLIM)
Disk (CLIM-Attached)	IOMF2	SNDA
Disk (Fibre Channel)	LIF	SSAC
Disk (SAS)	Logical Processor	Storage Router
DVD-ROM	Maintenance PIC	SWAN / SWAN2
E4SA	Maintenance Switch	SWAN Battery
EMU	Memory Card (Blade)	SWAN CLIP
Enclosure (Blade)	Module	SWAN Collection
ESS Disk	Monitored Service LAN Devices	SWAN Fan
ESS Disk Collection	NIC (CLIM)	SWAN LANLB
External Disk	Optical Extender PIC	SWAN Line
External Disk Collection	PCI Riser (CLIM)	SWAN Path
Fan	PIC	SWAN Power Supply
Fan Assembly	PIF	System
Fan (CLIM)	PMCU	Tape
Fan (IOAM)	Power Supply	Tape Collection
Fan (Processor Switch)	Power Supply (Blade Element)	TRSA
Fan (SAS Disk Enclosure)	Power Supply (CLIM)	Unknown
Fan (VIO)	Power Supply (FCDM)	UPS

FC Card (CLIM)	Power Supply (IOAM)	VIO FCSA
FC-AL I/O Module	Power Supply (Processor Switch)	VIO G4SA
FCDM	Power Supply (SAS Disk Enclosure)	VIO Logic Board
FCDM Collection	Power Supply and Fan (Telco SAS Disk Enclosure)	VIO Module
FCSA	Power Supply (VIO)	
FCSA FSAC	Processor (CLIM)	

4PSE (4-Port ServerNet Extender)

Used only in HP Integrity NonStop NS14000 or NonStop NS1000 systems containing IOAMs, 4PSEs provide ServerNet connectivity to the processors. Such systems contain just one IOAM enclosure with either one or two 4-Port ServerNet Extenders in each IOAM (in slots 1 and 2, in place of an FCSA or G4SA). Each 4PSE contains four [ports](#).

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether or not the 4PSE's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indicates whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Type	Identifies the type of ServerNet PIC. Value: 4-Port ServerNet Extender

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Power Off

Shuts off power to the 4PSE.

Power On

Restores power to the 4PSE.

Replace

Launches a service procedure describing how to replace a 4PSE.

Set LED State

Turns on or off the amber LED located on the 4PSE. The current state is indicated by the [LED State](#) attribute.

Alarm Panel (Telco)

For Telco systems only, this object can be displayed and monitored in OSM by using the [Start Monitoring Alarm Panel](#) action, located under the [Monitored Service LAN Devices](#) object. You can access its browser-based configuration interface through the [Link to Web Interface](#) action.

Location in OSM Tree: System > Monitored Service LAN Devices > Alarm Panel

Attributes

Alarm Panel

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Device Status	The state of the component as known to the operating system on the server.
Firmware Revision	The version of the firmware running on the alarm panel.
Hardware Revision	The hardware version of the alarm panel.
IPv4 Address	The IPv4 address of the alarm panel.
LED Manager Communication State	Indicates whether the alarm panel has lost communication with the manager that controls its LEDs. The possible values of this attribute are OK, Fault, and Unknown.
MAC Address	The media access control (MAC) address of the alarm panel.
Microprocessor State	Indicates whether the alarm panel microprocessor is in a good state (passed POST). The possible values of this attribute are OK, Fault, and Unknown.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power Input A State	The state of the power in input A of the alarm panel. The possible values of this attribute are OK, Fault, and Unknown.
Power Input B State	The state of the power in input B of the alarm panel. The possible values of this attribute are OK, Fault, and Unknown.
Serial Number	A unique identification number assigned to each alarm panel in manufacturing.

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the alarm panel is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the alarm panel within the rack.

Actions

Link to Web Interface

Opens a Web interface that provides detailed device configuration and information for the alarm panel.

Rediscover

Causes OSM to refresh and reanalyze the object. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Stop Monitoring

Stops OSM from monitoring the alarm panel.

ATM3SA (ATM Adapter)

A customer-replaceable unit (CRU) that connects the ServerNet SAN inside a server to an Asynchronous Transfer Mode (ATM) network through a logical connection known as an ATM line. Each ATM CRU contains one [ATM line](#).

This Nonstop S-series component can be connected to a Nonstop NS-series system through an IOMF2 enclosure.

Slot Location: ATM CRUs can be located in slots 51, 52, 53, and 54 in IOMF or IOMF2 enclosures (service side).

Example: ATM3SA (12.1.53)

Attributes

ATM3SA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indication of whether the component is powered On or Off.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Dump Filename	The name of the file used to store dumps of the ATM CRU memory.
Physical Transmission Type	The type of transmission used by the ATM CRU. This might be either a standard, such as SONET, or a line speed, such as 155 Mbps.
MAC Address	The media access control (MAC) address of the ATM CRU.

Automatic Dump State	Indication of whether the ATM adapter software is automatically dumped to the specified dump file if the software abends abnormally. Enabled: The software is automatically copied. Disabled: The software is not automatically copied. Unknown:: The Automatic Dump state could not be read.
Media Type	The type of media or cable, such as single-mode fiber or coaxial cable, supported by the ATM CRU.
Automatic Firmware Update	Indication of whether the ATM CRU firmware is automatically updated when the ATM CRU is started. The automatic firmware update occurs if either the Start action is performed through the OSM software or the START ADAPTER command is issued from SCF. Enabled: The firmware is automatically updated. Disabled: The firmware is not automatically updated. Unknown:: The Automatic Firmware Update state could not be read.
Device State	The state of the component as known to the operating system on the server. Values
Automatic Reload State	Indication of whether the ATM CRU software is automatically reloaded if the adapter software terminates abnormally. Enabled: The software is automatically reloaded. Disabled: The software is not automatically reloaded. Unknown:: The Automatic Reload state could not be read.
Download Filename	The name of the file used to download the ATM CRU adapter.
Processor Access List	The currently available processors that can access the adapter.

Firmware

Version	The version of the firmware running on the ATM CRU.
Default Firmware Filename	The name of the file to be used for a firmware update.
Default Firmware File Version	The version of the firmware to be used for a firmware update.
Compare State	Indication of the differences, if any, between the current and default firmware versions. Values

Actions

Abort

Terminates operation of the ATM CRU and the associated ATM line. When the Abort action finishes, the ATM CRU and the ATM line are in the Stopped state.

Firmware Update

Updates the ATM adapter firmware.

Responsive Test

Verifies that the component is connected and responding.

Start

Starts the ATM CRU and the associated ATM line. The ATM CRU must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the ATM CRU. When the Start action finishes, the ATM CRU and the ATM line are in the Started state.

Test Verify

Runs all the firmware diagnostic tests on the CRU. This test takes about three minutes to finish. The CRU must be in the Stopped state before you initiate the Test Verify action.

ATM Line

The Asynchronous Transfer Mode (ATM) line represents the logical link between the ATM CRU and the ATM network. There is one ATM line per [ATM CRU](#).

This Nonstop S-series component can be connected to a Nonstop NS-series system through an IOMF2 enclosure.

Location in OSM Tree: System > Group > Module > ATM3SA > Line

Example: Line \$ATM (1.1.54)

Attributes

Line \$ATM

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Maximum Number of VPCs	The maximum number of virtual path connections (VPCs). Value: 0 through 256
Maximum Number of VCCs	The maximum number of virtual channel connections (VCCs). Value: 0 through 3072
ATM Address Configured	The address that is specified for this ATM Line.
UNI Management Entity VPI	The User-Network interface (UNI) management entity virtual path identifier (VPI). Value: 0 through 255
Maximum Number of VCIs	The maximum number of Virtual Circuit IDs (VCIs) that can be active for permanent virtual circuits. Value: 32 through 3072
UNI Version	The version of the User-Network Interface (UNI) supported by this ATM line.
Maximum Number of VPIs	The maximum number of virtual path identifiers (VPIs) for permanent virtual circuits. Value: 0 through 256
ATM Address Registered	The address that is registered for this ATM Line.
Device State	The state of the component as known to the operating system on the server. Values
Maximum Number of VCI Bits	The address width and the maximum number of Virtual Circuit ID (VCI) bits that can be active. Value: 0 through 16
UNI Management Entity VCI	The User-Network interface (UNI) management entity virtual circuit identifier (VCI). Value: 0 through 3071
Maximum Number of VPI Bits	The address width and the maximum number of Virtual Path ID (VPI) bits that can be active. Value: 0 through 8

Actions

None.

Battery

The battery customer-replaceable unit (CRU), located in Nonstop S-series processor or I/O enclosures, is an assembly of 24 cells rated at 2.5 amp-hours per cell. The batteries are designed to handle occasional power failures that might occur at typical computer sites. Each processor or I/O enclosure contains two batteries.

Location in OSM Tree: System > Group > Module > Battery

Slot Location: In processor enclosures, battery CRUs are located in slots 23 and 28 (appearance side).

Example: Battery (1.1.28)

Attributes

Battery

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Power State	Indication of whether the component is powered on. Values

Logical

Charge State	The condition of the battery CRU. Fully Charged: The battery is fully charged. Charging: The battery is in the process of being charged. Critical: The battery needs recharging or replacement. Unknown: The battery is not responding, and its state cannot be determined.
Enabled State	The initial state of the power supply CRU at the time of discovery. Values

Upper Voltage Sensor

Current Value	The current voltage of the upper twelve cells of the battery.
---------------	---

Lower Voltage Sensor

Current Value	The current voltage of the lower twelve cells of the battery.
---------------	---

Differential Voltage Sensor

Current Value	The current voltage difference between the upper and lower cells of the battery.
---------------	--

Total Voltage Sensor

Normal Minimum Value	The minimum voltage that the battery should maintain is 42 volts. If the battery's Total Voltage falls below 42 volts, an alarm is generated. (If the Total Voltage falls below the Disconnect Voltage Limit of 39.6 volts, the battery is disconnected.)
Lower Fatal Threshold	The minimum voltage that the battery must maintain to continue operating is 39.6 volts. If the battery's Total Voltage falls below 39.6, the battery is disconnected. This disconnection could cause an enclosure or the entire system to go down.
Current Value	The current combined voltage of both the upper and lower cells of the battery. — If the Total Voltage falls below 42 volts, an alarm is generated. — If the Total Voltage falls below the 39.6 volts, the battery is disconnected.
Normal Maximum Value	The maximum voltage that the battery can hold (60 volts).

Actions

Enable/Disable

Prepares the battery to supply power when AC power is unavailable. The battery must be enabled to remain charged.

Parameter: Enabled (true = enabled, false = disabled)

Blade Complex

The Blade Complex object (formerly known in OSM as the Processor Complex) contains these NonStop NS-series processor components:

- A set of one, two, or three [Blade Elements](#), depending on system type and configuration. NonStop NS14000 series and NS16000 series servers can have two or three Blade Elements per Blade Complex, all other NS-series servers are limited to one.
- Four [Logical Processors](#) and their [Processor Components](#) (which, for NonStop NS14000 series and NS16000 series servers, includes their associated LSUs).

Attributes

Blade Complex

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Activity	Displayed only if there is an activity in progress, to report the current activity, such as Firmware Update in Progress or Service Procedure in Progress. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.
Activity Start Time	The time the current activity began. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.
Activity in Progress	If yes, displays the Activity and Activity Start Time attributes. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.

Expected Processor Redundancy	The expected redundancy for all the processors in the complex. Set using the Set Processor Expected Redundancy action. Values: Simplex, Duplex, Triplex NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.
Group Number	The Group Number for the Blade Complex.

Actions

These actions apply to NonStop NS14000 series and NS16000 series servers only. There are no actions under the Blade Complex object for any other NonStop servers.

Clear Activity in Progress

Clears the current service activity.

Firmware Update

Launches a guided procedure to update the firmware in the Blade Elements within the Blade Complex for Integrity NonStop NS14000 series and NS16000 series servers. Blade firmware for other types of NonStop NS-series servers is done through a Firmware Update action the [Blade Element](#) object.

Perform Cable Check

Initiates a complex-wide cable check.

Set Activity in Progress

Sets the current service activity.

Set Processor Expected Redundancy

Sets the expected redundancy for all the processors in the complex. Options are Simplex, Duplex, or Triplex.

Blade Element

Formerly known in OSM as a Slice, this physical entity in the [Blade Complex](#) consists of a chassis, processor board containing one or more processor elements (each supporting different [Logical Processors](#)) and memory, I/O interface board, midplane, optics adapters, fans, and [power supplies](#). The assembly is designed to be mounted in a 19-inch rack.

When a Blade Complex has multiple Blade Elements, they are identified in the OSM tree pane as 400.1, 400.2, and 400.3. In the Attributes tab, the Serial Number attribute translates those values to A, B, and C.

What OSM displays under the Blade Element object depends on the type of your HP Integrity NonStop server.

For NonStop NS14000 series and NS16000 series servers, OSM displays:

- Two [Blade Element Power Supply](#) objects.
- A [Blade Element Firmware](#) object.

For NonStop NS1000, NS1200, NS2000 series, NS5000, or NS3000AC servers (except where noted), OSM displays:

- A [Blade System Board](#) object (not applicable for NS5000 servers).
- A [DVD-ROM](#) object.
- A [ServerNet Interface Card](#) object.

- Two [Blade Element Power Supply](#) objects.
- [Fan Assembly](#) objects to represent each fan in the Blade as follows: slots 16 through 19 for NS1000, slots 16 through 20 for NS5000, and slots 33 through 44 for NS3000AC, NS1200, and NS2000 series.
- [Memory Card](#) objects.

For NonStop NS2100, NS2200 series, NS2300, and NS2400 series servers, OSM displays:

- Two [Blade Element Power Supply](#) objects.
- Six [Fan Assembly](#) objects to represent each fan in the Blade slots 32 through 37.
- [Memory Card](#) objects.

Attributes

Blade Element

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Fan Assembly (Slot 17) Status	Status of the Blade Element fan located in slot 17. Possible values include OK, Fault, Down. NOTE: Displayed for Integrity NonStop NS14000 series and NS16000 series servers only. For other NonStop NS-series servers, fan status is reported under the Fan Assembly objects.
Fan Assembly (Slot 18) Status	Status of the Blade Element fan located in slot 18. Possible values include OK, Fault, Down. NOTE: Displayed for Integrity NonStop NS14000 series and NS16000 series servers only. For other NonStop NS-series servers, fan status is reported under the Fan Assembly objects.
Fan Assembly (Slot 19) Status	Status of the Blade Element fan located in slot 19. Possible values include OK, Fault, Down. NOTE: Displayed for Integrity NonStop NS14000 series and NS16000 series servers only. For other NonStop NS-series servers, fan status is reported under the Fan Assembly objects.
Hardware Revision	Identifies the generation of the component. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.
Memory Reintegration Board Revision	The version of the memory/reintegration board in the Blade Element. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. NOTE: Not displayed for NonStop NS2100, NS2200 series, NS2300, and NS2400 series servers.
Serial Number	The serial number of the Blade Element.
Track ID	Unique identifier for each Blade Element, including an A, B, or C to indicate position within a Blade Complex.

Disk Boot Firmware Running Version	The version of the Disk Boot firmware currently running on the processor Blade Element. NOTE: Not applicable for NonStop NS14000 series and NS16000 series servers, where the firmware information is reported under the Blade Element Firmware object.
Halted State Services Firmware Running Version	The version of the HSS firmware currently running on the processor Blade Element. NOTE: Not applicable for NonStop NS14000 series and NS16000 series servers, where the firmware information is reported under the Blade Element Firmware object.
ISP1040 Firmware Running Version	The version of the ISP1040 firmware currently running on the processor Blade Element. NOTE: Not applicable for NonStop NS14000 series and NS16000 series servers, where the firmware information is reported under the Blade Element Firmware object.

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the Blade Element is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the Blade Element within the rack.
Locator	An optional text string assigned to further identify the physical location of the Blade Element. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical Location action. This attribute is displayed only if a value is specified through the action.

Actions

Check If Safe to Replace

Available for NonStop NS14000 series and NS16000 series servers only, this action indicates whether connectivity to the logical processor will be lost if the Blade Element is brought down or replaced.

Check Reintegration Status

Available for NonStop NS14000 series and NS16000 series servers only, this action checks to see whether or not the processor elements on this blade element are integrated to their corresponding logical processors. The action passes only if all PEs are reintegrated. Also, the action fails if the blade element is currently the source of reintegration for another blade element in the complex.

Clear Forward Progress Log

Clears the Forward Progress Log (FPL), which is more detailed than the System Event Log.

Disable Blade Element Reintegration

Available for NonStop NS14000 series and NS16000 series servers only, this action disables automatic reintegration of the Blade Element for 60 minutes.

Enable Blade Element Reintegration

Available for NonStop NS14000 series and NS16000 series servers only, this action enables automatic reintegration of the processor elements on this Blade Element in case of failure.

Firmware Update

This action, displayed for most Integrity NonStop servers, launches a documented service procedure for updating the Blade Element firmware. For NonStop NS14000 series and NS16000 series servers, the firmware update guided procedure is launched from the [Blade Complex](#) object instead.

Power Down Blade Element

For Integrity NonStop NS-series systems, this action effectively disconnects this Blade Element from the system and puts the Blade Element into low power mode, enabling it to be serviced.

- For NonStop NS14000 series and NS16000 series servers, the Blade Element remains in low power mode for 5 minutes.
- For NonStop NS1000, NS1200, NS2000 series, NS5000, and NS3000AC servers, this action powers off the Blade Element until such time as it is powered on manually (by pressing the power button on the Blade Element itself).
- For NonStop NS2100, NS2200 series, NS2300, and NS2400 series servers, the Blade Element is not powered down, but the action detail provides the IP address of the iLO that can be used to power it down.

NOTE: It is recommended that the power cables be disconnected once the Blade Element is in low power mode and before servicing the Blade Element.

Propagate System Name

Available for NonStop NS14000 series and NS16000 series servers only, this action propagates the current system name to all Blade Elements. (You are directed to use this action when a system name mismatch alarm occurs.)

Replace

Displays a procedure for replacing the Blade Element or other field-replaceable Blade Element components (except for power supply unit, which is launched by a Replace action on the Blade Element Power Supply object).

Reset Blade Element

Performs a power cycle on the Blade Element, after which the processor must be reloaded.

Retrieve and Clear BMC Event Log

Allows you to retrieve and save a raw Baseboard Management Controller (BMC) event log file and then clear the BMC event log.

Retrieve and Clear BMC Event Log - Formatted

Allows you to retrieve and save a formatted version of the Baseboard Management Controller (BMC) event log and then clear the BMC event log.

NOTE: With T0682 AAN and later, OSM saves a copy of each Blade Element's BMC event log to a file in \$system.zservice and clears the BMC event log daily between 1 and 2 a.m. The log file name is the format blMMMSDD, where MMM is Blade Element's module number, S is slot number, and DD is date of the month.

Retrieve Forward Progress Log

Retrieves the Forward Progress Log (FPL), which is more detailed than the System Event Log.

NOTE: This action can take up to an hour to complete.

Save Extended Inventory

Allows you to save a file containing an inventory of the Blade Element.

Set LED State

Available for NonStop NS14000 series and NS16000 series servers only, this action allows you to set the Blade Element front or rear (service side) amber LEDs to On or Off.

Set Locator LED State

Allows you to set the Blade Element locator LED to On or Off. For rx2620, On causes the locator LED to blink. For rx2660 blades and rx2800 i2 blades, On causes the locator LED to remain on continuously.

Set Optics Adapter LED State

Available for NonStop NS14000 series and NS16000 series servers only, this action allows you to set the Blade Element optics adapter amber or SFP LEDs for a particular PE LID (0, 1, 2, or 3) to On or Off.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the Blade Element:

- Rack Name is a user-defined name for the rack containing the Blade Element. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the Blade Element within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action fails.
- Locator is an optional text string to help identify the physical location of the Blade Element. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. An system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system, while creating a physical view of your modular racks.

Switch to Use Shadow Firmware Image After Reset

Available for NonStop NS14000 series and NS16000 series servers only, this action causes the Blade Element to start running the Baseboard Management Controller (BMC) firmware version that what was on the Shadow image at the time the action was initiated. For all other Blade Element firmware, this action sets the [NSBE Image After Next Reset](#) attribute values to Shadow, indicating that the current Shadow firmware image will be used after the next Reset action. Typically, you would first update the Shadow image (using the guided procedure launched by the Firmware Update action on the Processor Complex object), use this action to specify the Shadow image

following Reset, and perform the Reset to start running the new (non-BMC) firmware. Then you can update the other image, which was the Running image but, following the Switch to Use Shadow... and Reset actions, is now the Shadow image.

Switch to Use Running Firmware Image After Reset

Available for NonStop NS14000 series and NS16000 series servers only, this action sets the [NSBE Image After Next Reset](#) attribute value to Running, indicating that the current Running firmware image will be used after the next Reset action.

Blade Element Firmware

This object exists in OSM to display the many firmware attributes that exist for Integrity NonStop NS14000 series and NS16000 series [Blade Elements](#).

For these types of systems, the Blade Element firmware is updated through a guided procedure launched by the [Firmware Update](#) action located under the [Blade Complex](#) object. For duplex or triplex processor complexes, it is recommended that you update the Shadow image for all blade elements in the complex at the same time, then reset the blade elements one at a time (using the Reset Blade Element action under the Blade Elements object).

NOTE: For other Integrity NonStop servers, the firmware attributes valid for those systems are displayed under the [Blade Element](#) Physical attributes instead, and the update procedure is launched from a Firmware Update action located under the Blade Element object (rather than under the Blade Complex object).

Attributes

Blade Element Firmware

NSBE Image After Next Reset	NSBE represents NonStop Blade Element Firmware other than BMC . This attribute indicates whether the current Shadow or Running firmware image will be used following the next Reset action, as specified by using the Switch to Use Shadow or Running Firmware Image After Reset actions.
BMC Image After Next Reset	This attribute always displays a value of Running, because the Switch to Use Shadow Firmware Image After Reset action immediately causes the Blade Element to start running BMC firmware from the Shadow image. The Shadow image at the time the action is performed immediately becomes the Running image.

Halted State Services Firmware

Running Version	The version of the HSS firmware currently running on the processor Blade Element .
Shadow Version	The version of the HSS firmware currently designated as the Shadow image of the Blade Element firmware.
Default File Name	The name of the file to be used for a HSS firmware update.
Default File Version	The version of the firmware to be used for a HSS firmware update.
Running Compare State	The difference, if any, between the current Running image and default HSS firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default HSS firmware version. Values

Primitive State Firmware

Running Version	The version of the Primitive State firmware currently running on the processor Blade Element .
Shadow Version	The version of the Primitive State firmware currently designated as the Shadow image of the Blade Element firmware.
Default File Name	The full path name of the default Primitive State firmware file on the server.
Default File Version	The version of the firmware to be used for a Primitive State firmware update.
Running Compare State	The difference, if any, between the current Running image and default Primitive State firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default Primitive State firmware version. Values

Disk Boot Firmware

Running Version	The version of the Disk Boot firmware currently running on the processor Blade Element .
Shadow Version	The version of the Disk Boot firmware currently designated as the Shadow image of the blade element firmware.
Default File Name	The name of the file to be used for a Disk Boot firmware update.
Default File Version	The version of the firmware to be used for a Disk Boot firmware update.
Running Compare State	The difference, if any, between the current Running image and default Disk Boot firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default Disk Boot firmware version. Values

ISP1040 Firmware

Running Version	The version of the ISP1040 firmware currently running on the processor Blade Element .
Shadow Version	The version of the ISP1040 firmware currently designated as the Shadow image of the blade element firmware.
Default File Name	The name of the file to be used for a ISP1040 firmware update.
Default File Version	The version of the firmware to be used for an ISP1040 firmware update.
Running Compare State	The difference, if any, between the current Running image and default ISP1040 firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default ISP1040 firmware version. Values

Baseboard Management Controller Firmware

Running Version	The version of the BMC firmware currently running on the processor Blade Element .
Shadow Version	The version of the BMC firmware currently designated as the Shadow image of the blade element firmware.
Default File Name	The name of the file to be used for a BMC firmware update.
Default File Version	The version of the firmware to be used for a BMC firmware update.

Running Compare State	The difference, if any, between the current Running image and default BMC firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default BMC firmware version. Values

PAL/SAL Firmware

Running Version	The version of the PAL/SAL firmware currently running on the processor Blade Element .
Shadow Version	The version of the PAL/SAL firmware currently designated as the Shadow image of the blade element firmware.
Default File Name	The version of the firmware to be used for a PAL/SAL firmware update.
Default File Version	The version of the HSS PAL/SAL firmware to be used for a firmware update.
Running Compare State	The difference, if any, between the current Running image and default PAL/SAL firmware version. Values
Shadow Compare State	The difference, if any, between the current Shadow image and default PAL/SAL firmware version. Values

Actions

None

Blade System Board

In the OSM Service Connection, an object displayed as a subcomponent under the Blade Element object for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, and NS3000AC servers only.

Attributes

Blade System Board

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
-------------	---

Actions

None

Blower (FCDM)

A subcomponent of an [FCDM](#).

There are two blowers in each FCDM. Each blower is mounted on a power supply and cools the enclosure by circulating air through the enclosure and the elements. The rate at which air moves (the air flow) determines the amount of cooling and is a function of blower speed (rpm). These blowers, under the control of the EMU or the associated power supply, can operate at multiple speeds. This ensures that when the enclosure temperature changes the blowers can automatically adjust the air flow.

Location in OSM Tree: System > Group > FCDM Collection > FCDM > Blower

Example: Blower (111.211.1.97)

Attributes

Blower

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

LED State	Indicates whether or not the blower's (amber) fault LED is blinking. Value: Blinking or Off
Type	The vendor hardware type.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	---

Actions

Blink LED Off

Turns off the blinking of the blower's (amber) fault LED.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED OFF

Blink LED On

Causes the blower's (amber) fault LED to start blinking.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED ON

Replace

Displays the procedure for replacing the blower.

CCSA (Common Communication ServerNet Adapter)

An adapter that allows PCI-based communications devices to connect to a server. A CCSA CRU can hold up to four CCSA ServerNet addressable controllers ([SACs](#)) with four ports each, providing up to 16 links per adapter.

This Nonstop S-series component can be connected to a Nonstop NS-series system through an IOMF2 enclosure.

Location in OSM Tree: System > Group > Module > CCSA

Example: CCSA \$ZZLAN.CCSA1 (2.1.53)

Attributes

CCSA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indication of whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the Common Communication ServerNet adapter (CCSA) CRU and its associated ServerNet addressable controller (SAC). When the Abort action finishes, the CCSA CRU and SAC are in the Stopped state.

Start

Starts the Common Communication ServerNet adapter (CCSA) CRU and its associated ServerNet addressable controller (SAC). The CCSA CRU and the SAC must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the SAC. When the Start action completes, both the CCSA CRU and SAC are in the Started state.

Stop

Rather than automatically stopping the CCSA (as the Abort action does), this action first warns you if the CCSA is currently in use (and stops it only after you confirm).

Test Verify

Checks the health of the Common Communication ServerNet adapter (CCSA) CRU. It determines whether the CCSA CRU can communicate with at least one SAC on the board.

CLIM

In the OSM Service Connection, a CLIM object represents each CLuster I/O Module (CLIM) connected to a NonStop BladeSystem or supported NonStop NS-series system. CLIMs are configured initially in the OSM Low-Level Link, then by using the [Configure CLIM](#) action. CLIM software updates – both basic CLIM software and INS software (for Telco only) – are done in the OSM Low-Level Link.

For each CLuster I/O Module (CLIM), the OSM Service Connection displays these subcomponents, depending on whether it is a Storage CLIM or an IP CLIM:

- [DIMM](#)
- [Fan](#)

- FC Card
- Hard Disk
- InfiniBand HCA Card (G6 CLIMs only)
- Motherboard (G6 and Gen8 CLIMs only)
- NIC
- PCI Riser
- Power Supply
- Processor
- SAS Card
- ServerNet Interface Card
- Smart Array Controller (G6 and Gen8 CLIMs only)

To update firmware on CLIM components, you can use the actions located on the individual component objects within the OSM Service Connection or the Down System CLIM Firmware Update Tool.

The Down System CLIM Firmware Update Tool is installed on NonStop system consoles as part of the OSM Console Tools product T0634 G06 ABB and later. It is launched from the Windows Start menu by selecting All Programs > HP OSM > Down System CLIM Firmware Update Tool. In order to perform firmware updates through the Down System CLIM Firmware Update Tool, you must first perform the Prepare for Down System CLIM Firmware Update action, located under the [CLIMs](#) object, then bring the system down.

Location in OSM Tree: System > CLIMs > CLIM

Attributes

CLIM

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

CIP Software Version	The version of the CIP software running on the CLIM.
Configured Connections per ServerNet Fabric	Displays a value of 1 or 2, as specified in the Configure CLIM action, depending on whether there are one or two physical connections between a CLIM and a P-switch (NS-series) or ServerNet switch (Integrity NonStop BladeSystem).
Configured Operation Mode	Displays whether the CLIM will be used for IP, Storage, or Open (Telco), as specified in the Configure CLIM action.
Connection Status	Displays the status of the connection.
Device State	The state of the CLIM as a result of the operator command issued via OSM or SCF. Possible values include Stopped, Starting, and Started.
Down Physical Network Interfaces	List of physical Ethernet interfaces on the CLIM that are down.
IP Software Version	The version of the IP software running on the CLIM.
Linux Version	The version of the Linux software running on the CLIM.
Maintenance Interface IPv4 Address	The IPv4 address used to connect directly to the CLIM.

Registered with Key Managers	This attribute applies only to supported storage CLIMs (G5 and later), and indicates whether or not – at the time of discovery – the CLIM had been successfully registered to the Key Manager or Key Manager Cluster using the Register CLIMs with Key Managers guided procedure.
Storage Software Version	The version of storage software running on the CLIM.
Temperature Status	Indicates whether or not the CLIM has exceeded its temperature threshold for proper operation. The possible values are “Temperature sensing not supported by this system,” “Normal,” “Degraded,” and “Critical.” If the value is not available, this attribute is not displayed.
Up Physical Network Interfaces	List of physical Ethernet interfaces on the CLIM that are operational.
X1 Fabric Connection State X2 Fabric Connection State	<p>The connectivity status of the CLIM to the ServerNet X fabric. Displayed for both X1 and X2 fabrics, provided the CLIM is configured for two connections per ServerNet fabric. Possible values include:</p> <ul style="list-style-type: none"> • Correctly Connected: The CLIM is correctly connected to the ServerNet X fabric. • Not Connected: The CLIM is not connected to the ServerNet X fabric. • Location Mismatch: The CLIM is configured to be connected to a p-switch, but is connected to a different port. • System Name Mismatch: The CLIM is configured with a system name that does not match the name of the system to which it is connected. • Operation Mode Mismatch: The operation mode does not match with the configured operation mode. • Number of Connections per ServerNet Fabric Mismatch: The number of connections per ServerNet fabric does not match with the configured number. • Port Not Configured for CLIM: The p-switch is not configured to be connected to a CLIM. • Unsupported Location: the configured location is not supported for connection with a CLIM. • Unknown: The system is unable to determine the connection state of the CLIM on this fabric.
Y1 Fabric Connection State Y2 Fabric Connection State	<p>The connectivity status of the CLIM to the ServerNet Y fabric. Displayed for both Y1 and Y2 fabrics, provided the CLIM is configured for two connections per ServerNet fabric. Possible values include:</p> <ul style="list-style-type: none"> • Correctly Connected: The CLIM is correctly connected to the ServerNet Y fabric. • Not Connected: The CLIM is not connected to the ServerNet Y fabric. • Location Mismatch: The CLIM is configured to be connected to a p-switch, but is connected to a different port. • System Name Mismatch: The CLIM is configured with a system name that does not match the name of the system to which it is connected. • Operation Mode Mismatch: The operation mode does not match with the configured operation mode. • Number of Connections per ServerNet Fabric Mismatch: The number of connections per ServerNet fabric does not match with the configured number. • Port Not Configured for CLIM: The p-switch is not configured to be connected to a CLIM. • Unsupported Location: the configured location is not supported for connection with a CLIM. • Unknown: The system is unable to determine the connection state of the CLIM on this fabric.
iLO DNS Name	The DNS name of the Integrated Lights Out (iLO) on the CLIM.

iLO IPv4 Address	The IPv4 address of the Integrated Lights Out (iLO) port on the CLIM. The IP address of the CLIM iLO is displayed only when SNMP is available; however, the iLO DNS Name attribute is displayed even when SNMP is not available.
iLO Pulse Link State	Possible values: Up or Down.

Physical

Model	The model number of the CLIM that was assigned in manufacturing.
Part Number	The part number of the CLIM that was assigned in manufacturing.
Serial Number	The serial number of the CLIM.

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the CLIM is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the CLIM within the rack.

X1 Fabric Information

Configured Location	The location of the ServerNet X1 fabric port where the CLIM is configured. Example: Group 100, Module 2, Slot 5, Port 3, Fiber 1 (Fiber applies to NonStop BladeSystems only)
---------------------	---

X2 Fabric Information

Configured Location	The location of the ServerNet X2 fabric port where the CLIM is configured, provided the CLIM is configured for two connections per ServerNet fabric. Example: Group 100, Module 2, Slot 7, Port 3, Fiber 2 (Fiber applies to NonStop BladeSystems only)
---------------------	---

Y1 Fabric Information

Configured Location	The location of the ServerNet Y1 fabric port where the CLIM is configured. Example: Group 100, Module 3, Slot 5, Port 3, Fiber 1 (Fiber applies to NonStop BladeSystems only)
---------------------	---

Y2 Fabric Information

Configured Location	The location of the ServerNet Y2 fabric port where the CLIM is configured, provided the CLIM is configured for two connections per ServerNet fabric. Example: Group 100, Module 3, Slot 7, Port 3, Fiber 2 (Fiber applies to NonStop BladeSystems only)
---------------------	---

iLO

Version -- the version of the firmware running on the iLO.

Compare State	Indication of the differences, if any, between the current and default iLO firmware versions. Values
Default File Name	The name of the file to be used for an iLO firmware update.

Default File Version	The version of the firmware to be used for an iLO firmware update.
Version	The version of the firmware running on the iLO.

ROM

Version -- the version of the ROM firmware running on the CLIM.

Compare State	Indication of the differences, if any, between the current and default ROM firmware versions. Values
Default File Name	The name of the file to be used for an ROM firmware update.
Default File Version	The version of the firmware to be used for an ROM firmware update.
Version	The version of the ROM firmware running on the CLIM.

Actions

Backup CLIM Configuration

Backs up the CLIM configuration to location to a file at a user-specified location, or to a default location, if one is not provided by the user.

Collect CLIM Logs

Finds and collects CLIM logs, saving them to a subvolume location on the NonStop system specified through the [Set Location for CLIM Log Collection](#) action. If no location is specified, a default location of \$system.zservice will be used. Rediscovery of the system or even the CLIMs object returns the location to the default value, so it will be necessary to perform the Set Location for CLIM Log Collection action again before performing the Collect CLIM Logs action if you wish to use a location other than the default.

Delete

OSM issues a SPI command equivalent to SCF DELETE CLIM to CIPMAN.

iLO Update

Updates the firmware on the iLO card. Upon specifying the location of the firmware file, OSM uses TACLPRVD to SFTP the firmware file to the CLIM, then uses the command-line `climcmd` command to update the firmware on the specified card. If a firmware file location is not specified, the default iLO firmware file location will be used.

Invoke iLO

Invokes the Integrated Lights Out (iLO) web-based interface to the specified CLIM using the iLO IP address or DNS name of the CLIM iLO. The iLO interface will then prompt you for an iLO username and password.

Reboot

OSM issues a reboot command on the CLIM. A dialog box provides you with the option to perform a dump of diagnostic data before rebooting the CLIM. The default value of "Yes" performs the diagnostic data collection, and saves the data file to the /home/debuginfo directory on the CLIM. Choosing "No" performs the reboot without collecting diagnostic data.

Replace

Launches a guided procedure to make replacement of a CLIM more automated.

Replace Hard Drive

Launches a guided procedure to make replacement of a CLIM hard disk drive more automated. This guided procedure can also be launched through the [Replace](#) action on the (CLIM) Hard Disk object, although CLIM subcomponents, such as the Hard Disk object will not be displayed by OSM if SNMP is not available.

Restore CLIM Configuration

Restores the CLIM configuration from a previously saved file at a user-specified or default location.

Restore Default Storage Path Configuration

Valid for Storage CLIM only. OSM issues a SPI command to the storage subsystem to restore the active paths of all storage devices using the CLIM to their default configurations.

ROM Update

Updates the ROM firmware. Upon completion, OSM offers to reboot the CLIM, in order for the CLIM to start using the updated firmware.

Set UID LED State

Turns the Unit Identification LED on or off to aid in the physical identification of a CLIM by means of that blue light on the front or back of the CLIM.

Show CLIM/Key Manager Registration Information

This action, applicable only for CLIMs that have been registered through the [Register CLIMs with Key Managers](#) guided procedure, displays information concerning the registration of the CLIM with the Key Manager or Key Manager Cluster, including:

- Key Manager Cluster configuration, including tier assignment and IP addresses.
- Local CA certificate that signed the Server certificate.
- Client Certificate information.
- CLIM/Key Manager user name.

Start

OSM issues a SPI command to CIPMAN equivalent to SCF START CLIM.

Stop

Encompasses both the SCF STOP and ABORT commands. OSM issues a SPI command to CIPMAN equivalent to SCF STOP CLIM. If this fails because there are open sockets and you tell OSM to proceed any way, OSM issues a SPI command to CIPMAN equivalent to SCF ABORT CLIM, FORCED.

Stop Storage Paths

Valid for Storage CLIM only. Stops all storage paths from the CLIM.

Switch Storage Paths Away

Valid for Storage CLIM only. OSM issues a SPI command to the storage subsystem to switch the active paths of all storage devices using the CLIM away from the CLIM.

CLIMs

In the OSM Service Connection, CLIMs is a collection object that contains all [CLIM](#) (CLuster I/O Module) devices configured on a NonStop BladeSystem or supported NonStop NS-series system.

Location in OSM Tree: System > CLIMs

Attributes

None.

Actions

Collect CLIM Logs

This action finds and collects CLIM logs, saving them to a subvolume location on the NonStop system specified through the [Set Location for CLIM Log Collection](#) action. If no location is specified, a default location of \$system.zservice will be used. Rediscovery of the system or even the CLIMs object returns the location to the default value, so it will be necessary to perform the Set Location for CLIM Log Collection action again before performing the Collect CLIM Logs action if you wish to use a location other than the default.

Configure CLIM

After you log on to and do initial CLIM configuration in the OSM Low-Level Link, this action, equivalent to the SCF ADD CLIM command, completes the CLIM configuration. During the action, OSM does not attempt to verify that an operational CLIM physically exists at the specified locations. However, once configured, if the CLIM is not physically attached, a Connection or Configuration Error alarm will be generated.

Upon initiating the action, a dialog box prompts you to enter the following:

- CLIM name – a name that will be displayed by the OSM Service Connection to identify the CLIM.
- Group, Module, Slot, and Port location of one of the P-switch or ServerNet switch ports to which the CLIM is or will be connected.
- Fiber – valid for NonStop BladeSystems only, enter a value of 1 to 4.
- Operation Mode – from a drop-down menu, specify whether the CLIM will be used for IP, Storage, or Open (Telco). This value will be displayed under the Configured Operation Mode attribute for the CLIM.
- Number of Connections per ServerNet Fabric – from a drop-down menu, specify the number of physical connections per ServerNet fabric that will be used to connect the CLIM to the NonStop system. The possible values are 1 and 2. The default value for IP and Open (Telco) CLIMs is 1; the default value for Storage CLIMs is 2. This value will be displayed under the Configured Connections per ServerNet Fabric attribute for the CLIM.
- Provider Name – if not specified, a default Provider will be used by the CIP subsystem. However, if you do specify a Provider name, it must have been already added on the system via the SCF ADD PROVIDER command before specified here. Otherwise, the Configure CLIM action will fail because the Provider specified does not exist.
- Multiple Provider Support – a drop-down menu from which you select ON or OFF to indicate whether or not this CLIM will be configured to support multiple providers.

Once you enter or update all required information and click **OK**, OSM issues a SPI command (equivalent to SCF ADD CLIM) to CIPMAN.

Prepare for Down System CLIM Firmware Update

This action is designed to be used only in conjunction with the Down System CLIM Firmware Update Tool and must be performed **before** using that tool. The Down System CLIM Firmware Update Tool can be used to update firmware/BIOS on the following CLIM components during planned system down time:

- CLIM iLO
- CLIM ROM

- CLIM Smart Array Controller
- CLIM NIC
- CLIM InfiniBand HCA
- CLIM SAS Firmware
- CLIM SAS BIOS
- CLIM FC Firmware
- CLIM FC BIOS
- SAS Disk Enclosure (but not individual SAS disk) Firmware

NOTE: The Down System CLIM Firmware Update Tool is installed on the NonStop system console as part of the OSM Console Tools product, T0634 G06 ABB and later. It requires SSH SPR T0801^ABA or later. For information on installing the Down System CLIM Firmware Update Tool, see the *NonStop System Console Installer Guide*. For instructions on using the Down System CLIM Firmware Update Tool, see the online help available from within the tool.

When installed on the NSC, it is launched from the Windows Start menu as follows:

Start > All Programs > HP OSM > **Down System CLIM Firmware Update Tool**

To perform the **Prepare for Down System CLIM Firmware Update** action, users must have OpenSSH access permissions. The default NSC users (Administrator, NSC_Administrator, and GCSC user accounts) automatically have those permissions configured when OpenSSH is installed on the console through the Master installer (as part of Console CLIM Utilities). You can specify a user other one of those default users when performing the action, but that user must first be configured on the NonStop system console as follows:

For a local user, execute the following command:

```
sshuser -s user-name -u user-name -f passwd-file
```

where:

user-name

is the NSC user name to be configured.

passwd-file

is the location of passwd file in etc directory under the OpenSSH installed directory; for example:
C:\Program Files\OpenSSH\etc\passwd.

For a domain user, execute the following command:

```
sshuser -s domain-name\user-name -u user-name -d domain-name -f  
passwd-file
```

where:

domain-name

is the name of the domain.

user-name

is the NSC user name to be configured.

passwd-file

is the location of passwd file in etc directory under the OpenSSH installed directory; for example:
C:\Program Files\OpenSSH\etc\passwd.

When you perform the **Prepare for Down System CLIM Firmware Update** action, a dialog prompts you to specify:

- The new SYSnn location to be used after the RVU upgrade.

NOTE: This location is the alternate SYSnn on which you installed the SUT containing the new firmware to be used for the update.

- The IP address of the NonStop system console to which the files will be transferred.
 - User name and password for the NSC.
-

NOTE: This user must have the necessary OpenSSH access permissions, as described above.

Click **OK** to proceed.

The Prepare for Down System CLIM Firmware Update action collects information on all CLIM firmware/BIOS components whose Compare State is not “Same” or “Compatible” and creates a list of the components that need to be updated. This list along with the actual firmware/BIOS binary files is transferred to specified NonStop System Console. The Down System CLIM Firmware Update Tool uses this information to perform the firmware/BIOS updates.

Register CLIMs with Key Managers

This action launches an OSM guided procedure of the same name, to guides you through the process of registering storage CLIMs with Key Managers for the purpose of providing volume level encryption on storage devices. Keys generated by the Key Manager help protect your storage data.

NOTE: For requirements and steps that must be performed **before** using this guided procedure, see the *NonStop Volume Level Encryption Guide*. For more information on using the guided procedure, see the online help available from within the procedure.

For each supported CLIM object, OSM displays a [Registered with Key Managers](#) attribute to indicate whether or not the CLIM has been successfully registered to the Key Manager or Key Manager Cluster using this guided procedure. There is also an action on the CLIM object to [Show CLIM/Key Manager Registration Information](#).

Set Location for CLIM Log Collection

This action allows you to specify a non-default location on the NonStop system for collecting CLIM logs through the [Collect CLIM Logs](#) action. Upon performing this action, a dialog box prompts you to specify a subvolume location in the form \$vol.subvol. Rediscovery of the system or even the CLIMs object returns the location to the default value, so it will be necessary to perform the Set Location for CLIM Log Collection action again before performing the Collect CLIM Logs action if you wish to use a location other than the default.

CLIM-Attached Disks

A collection object that represents all [disks](#) attached to [CLIMs](#) (CLuster I/O Modules) configured on a system.

Location in OSM Tree: System > CLIM-Attached Disks

Attributes

None.

Actions

None.

DIMM (CLIM)

A subcomponent of the [CLIM](#); details that vary according to CLIM type include:

- For G2 and G5 CLIMs, there are eight DIMM slots that can be populated.
- For G6 CLIMs, there are 18 DIMM slots that can be populated. Nine of those DIMM slots are associated with the processor installed in processor socket 1. The other nine DIMM slots are associated with the processor installed in processor socket 2. The location is identified in OSM by appending the processor number and slot to the DIMM name. For example, DIMM \$ZZCIP.C1002572.1.3 is in the slot 3 that is associated with processor 1; DIMM \$ZZCIP.C1002572.2.6 is in the slot 6 that is associated with processor 2.
- For Gen8 CLIMs, there are 12 DIMM slots, all on a single processor.

Location in OSM Tree: System > CLIMs > CLIM > DIMM

Attributes

DIMM

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the DIMM as known to the operating system on the server. Possible values include: OK, Degraded, Fault, Not Installed, Install Error.
Size	Total size of the DIMM in KB.

Actions

Replace

Launches a documented service procedure to replace a DIMM memory card in a CLIM.

Disk

An internal 3.5-inch hard disk drive. Each disk drive connects to one of two SCSI buses on an [IOMF2](#) CRU.

Disk CRUs can be located in slots 01 through 08 and slots 11 through 18 in I/O enclosures (appearance side). SCSI terminators are in slots 09, 10, 19 and 20, for a total of 16 available disk slots.

Location in OSM Tree: System > Group > Module > Disk

Example: Disk \$SYSTEM-P (1.1.11)

Attributes

Disk

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indication of whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Active Path	The path that is currently accessing the disk. Values: Primary, Backup, Mirror, Mirror Backup
Backup Path State	The current state of the backup disk path. Values .
Logical Device Number	The logical device number used by the operating system to identify the disk. Example: 7
Media Size	The total size (in kilobytes) of disk storage space.
Primary Path State	The current state of the primary disk path. Values .
Product ID	A unique number that identifies the product.

Process Pair

Configured Processors	The 2 processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296
Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285

Disk Pair

Disk Pair Name	The name and location of the mirrored disk. Example: Disk \$DATA00-M (1.1.2).
----------------	---

Firmware

Version	The version of the firmware running on the disk.
---------	--

Backup Path

Access State	The accessibility of the backup path. Example: Inactive, Active
Configured Controller Location	The location of the backup disk path SCSI controller. Example: PMF.SAC-2.GRP-1.MOD-1.SLOT-55
SCSI Controller	A number (1 or 2) that identifies the backup SCSI controller that manages the disk. Example: SCSI Controller (1.1.50.2)
SCSI ID	An identification number assigned to the device when configured.

Primary Path

Access State	The accessibility of the primary path. Values: Inactive, Active
Configured Controller Location	The location of the primary disk path SCSI controller. Example: PMF.SAC-2.GRP-1.MOD-1.SLOT-50
SCSI Controller	A number (1 or 2) that identifies the primary SCSI controller that manages the disk. Example: SCSI Controller (1.1.50.2)
SCSI ID	An identification number assigned to the device when configured.

Actions

Abort Backup Path

Terminates operation of the backup path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Backup Path action before you can start the path again.

Abort Disk

Terminates operation of all paths for the disk. When the Abort action finishes, the paths are in a Hard Down state. You must use the Reset Disk action before you can start the paths again.

Abort Primary Path

Terminates operation of the primary path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Primary Path action before you can start the path again.

Clear Data

Erases all data on the disk but leaves the disk label intact. Clear Data does not erase the FIR data in the CE sector, the volume label, the boot sector, or the spare tracks table. After a Clear Data completes or is cancelled, the disk drive is not usable until you restore the file system by using the SCF INITIALIZE DISK command.

The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

Firmware Update

Updates firmware for the selected disk.



CAUTION: Perform this action only when instructed to by service provider, Support Note, or other notification.

To update disk firmware:

1. Locate and transfer the appropriate firmware source file to your server. Disk firmware versions vary by manufacturer and model number. The correct version for one disk drive might not work for others.
2. Log on to the OSM Service Connection and use the Actions dialog box (to update one disk at a time) or the Multi-Resource Actions dialog box (to update multiple disks of the same type simultaneously).
3. Stop the disk or disks that you want to update.
4. Perform the **Firmware Update** action.
5. Click **OK** to the Confirm Firmware Update dialog box. This displays the Parameter Input.

NOTE: Contrary to the generic dialog text, for disk firmware you must specify the firmware source file path (established in Step 1). Because disk firmware versions vary, OSM does not use a default file name. If you do not specify a valid file path, the action fails.

6. Enter the firmware source file path (established in Step 1) and click **OK**.
7. Restart the disk or disks.

Power Off

Removes power to the disk drive.

Power On

Restores power to the disk drive.

Reset Backup Path

Places the backup path in a state from which it can be started.

Reset Disk

Places the disk in a state from which it can be started. This action might be necessary before starting a disk that has both paths in a Hard Down state; for example, if a hardware error has occurred, if the disk was stopped with an Abort action, or if a Stop or Abort fails to put the disk into the Down state.

If only one disk path is in a Hard Down state, you can use the [Reset Primary Path](#) or [Reset Backup Path](#) as appropriate.

Reset Primary Path

Places the primary path in a state from which it can be started.

Reset Volume

Places the volume in a state from which it can be started.

Responsive Test

Verifies that the disk drive is installed and responding.

Save as System Load Configuration

Specifies, within OSM, this disk as an alternate system load volume. For NonStop BladeSystem NB54000c and NB56000c only, if the action passes and a valid core license file is present in \$SYSTEM, OSM offers to copy the license file copied to each new alternate system disk.

You can specify up to four such alternate system load configurations. Each one is displayed under the system attributes in the OSM Service Connection and can be selected from within the System Load dialog box in the OSM Low-Level Link.

NOTE: With OSM Low-Level Link T0633 AAQ and later, you can also save system configuration files on the system console. Those saved configurations are not displayed as attributes values in the OSM Service Connection, but can be used during the system load operations in the Low-Level Link. For more information, see the OSM Low-Level Link online help.

Start Backup Path

Starts the backup path to this disk drive. When the Start action completes, the backup path is in the Started state.

This action fails if both paths to this disk are down and the mirrored disk is Up. For more information, see [Start Disk](#).

Start Disk

Use this action to start all paths to the disk drive only when:

- The disk paths are in a Down state. (Hard Down states require a reset action, either [Reset Disk](#), [Reset Primary Path](#), or [Reset Backup Path](#) as appropriate.)
- Its mirrored disk is not currently Up. The Start Disk action is designed to fail if the mirrored disk is already in an Up state because the mirror and primary disk volumes can have different data and require a revive operation. To revive and bring up the disks properly, use the OSM [Start Volume](#) action or SCF START DISK command.

When the action completes successfully, all paths to the disk are in the Started state.

Start Primary Path

Starts the primary path to this disk drive. When the Start action completes, the primary path is in the Started state.

This action fails if both paths to this disk are down and the mirrored disk is Up. For more information, see [Start Disk](#).

Start Volume

Starts all paths for both the primary and mirror drives of this volume unless they are in a Hard Down state. Disk paths in a Hard Down state require a reset action first (either [Reset Disk](#), [Reset Primary Path](#), or [Reset Backup Path](#) as appropriate).

Stop Backup Path

Terminates the backup path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Disk

Terminates all paths for this disk drive. When the Stop action finishes, the paths are in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Primary Path

Terminates the primary path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Volume

Terminates all paths for the primary and mirror drives of this volume. When the Stop action finishes, the paths are in a Down state.

Switch Process Pair

Switches the primary and backup disk I/O processes.

Switch to Backup Path

Switches processing from the primary to the backup path.

Switch to Primary Path

Switches processing from the backup to the primary path.

Test Verify

Runs the power-on self-test for the disk and tests the internal circuitry of the drive.

Validate Checksum

Scans the user data area of a disk for sector checksum errors. If the action fails, the Action Details dialog box reports a sector checksum and suggests that you spare the sector only if you believe there is a drive media problem.

To find additional information, use the OSM Event Viewer. Retrieve events using \$ZLOG as the source criteria and RAL as the subsystem criteria, and look for Disk-sector-failure events (event number 7001). In the event detail, a Sector-failure-count token shows how many sector checksum errors were found, and a Disk-logical-sector token appears for each error, providing the logical address of that failing sector.

You can perform the Validate Checksum action while the disk drive is in use. The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

Disk (CLIM-Attached)

Within the CLIM-Attached Disks object, the OSM Service Connection displays this Disk object as a logical representation of each CLIM-attached SAS or FC disk. A physical representation of each CLIM-attached SAS disk is displayed under the [SAS Disk Enclosure](#) object.

Location in OSM Tree: System > CLIM-Attached Disks > Disk

Attributes

Disk

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Active Path	The path that is currently accessing the disk. Values: Primary, Backup, Mirror, Mirror Backup
Backup Path State	The current state of the backup disk path. Values .
Disk Type	Indicates whether the disk is a SAS disk, Fibre Channel (FC), or SSD (solid state drive).
Encryption State	Displayed only if the system is licensed for NonStop Volume Level Encryption, this attribute indicates whether or not the CLIM to which the SAS disk is attached has NonStop Volume Level Encryption enabled.
Logical Device Number	The logical device number used by the operating system to identify the disk. Example: 7

Media Size	The total size (in kilobytes) of disk storage space.
Partition Number	The number of the partition on a partitioned disk.
Physical Location	The location of the physical disk that is mapped to this logical disk.
Primary Path State	The current state of the primary disk path. Values .
Product ID	A unique number that identifies the product.

Backup Path

Access State	Indicates whether the disk is active or inactive.
Configured CLIM	The CLIM to which the backup path is configured.
LUN	The logical unit number of the disk. Example: 101

Disk Pair

Disk Pair Name	The name and location of the mirrored disk. Example: Disk \$SAS25-M.
----------------	--

Primary Path

Access State	Indicates whether the disk is active or inactive.
Configured CLIM	The CLIM to which the primary path is configured.
LUN	The logical unit number of the disk. Example: 101

Process Pair

Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285
Configured Processors	The 2 processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296

Actions

Abort Backup Path

Terminates operation of the backup path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Backup Path action before you can start the path again.

Abort Disk

Terminates operation of all paths for the disk. When the Abort action finishes, the paths are in a Hard Down state. You must use the Reset Disk action before you can start the paths again.

Abort Primary Path

Terminates operation of the primary path to the disk. When the Abort action finishes, the path is in the Stopped state.

Clear Data

Available only for SAS or SSD disks – Erases all data on the disk but leaves the disk label intact. Clear Data does not erase the FIR data in the CE sector, the volume label, the boot sector, or the spare tracks table. After a Clear Data completes or is cancelled, the disk drive is not usable until you restore the file system by using the SCF INITIALIZE DISK command.

The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

Reset Backup Path

Places the backup path in a state from which it can be started.

Reset Disk

Places the disk in a state from which it can be started. This action might be necessary if the disk was in a STOPPED state, substate HARDDOWN; a hardware error has occurred; the disk was stopped with an ABORT command; or a STOP or ABORT fails to put the disk into the STOPPED state, substate DOWN.

Reset Primary Path

Places the primary path in a state from which it can be started.

Reset Volume

Places the volume in a state from which it can be started.

Responsive Test

Verifies that the disk drive is installed and responding.

Save as System Load Configuration

Specifies, within OSM, this disk as an alternate system load volume. For NonStop BladeSystem NB54000c and NB56000c only, if the action passes and a valid core license file is present in \$SYSTEM, OSM offers to copy the license file copied to each new alternate system disk.

You can specify up to four such alternate system load configurations. Each one is displayed under the system attributes in the OSM Service Connection and can be selected from within the System Load dialog box in the OSM Low-Level Link.

NOTE:

- This action will fail if performed on a partitioned disk.
 - With OSM Low-Level Link T0633 AAQ and later, you can also save system configuration files on the system console. Those saved configurations are not displayed as attributes values in the OSM Service Connection, but can be used during the system load operations in the Low-Level Link. For more information, see the OSM Low-Level Link online help.
-

Set LED State

Sets the LED on the physical disk in the SAS disk enclosure to On or Off.

Start Backup Path

Starts the backup path to this disk drive. When the Start action completes, the backup path is in the started State.

Start Disk

Starts all paths to this disk drive. When the Start action completes, all paths are in the Started state.

Start Primary Path

Starts the primary path to this disk drive. When the Start action completes, the primary path is in the Started state.

Start Volume

Starts all paths for both the primary and mirror drives of this volume.

Stop Backup Path

Terminates operation of the backup path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Disk

Terminates all paths for this disk drive. When the Stop action finishes, the paths are in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Primary Path

Terminates the primary path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Volume

Terminates all paths for the primary and mirror drives of this volume. When the Stop action finishes, the paths are in a Down state.

Switch Process Pair

Switches the primary and backup disk I/O processes.

Switch to Backup Path

Switches processing from the primary to the backup path.

Switch to Primary Path

Switches processing from the backup to the primary path.

Disk (Fibre Channel)

A Fibre Channel disk that resides in a Fibre Channel disk module (FCDM).

Location in OSM Tree: System > Group > FCDM Collection > FCDM > Disk

Example: Disk (111.211.1.3)

Attributes

Disk (Fibre Channel)

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Device State	The state of the component as known to the operating system on the server.
LED State	Indicates whether or not the disk drive's (amber) fault LED is blinking. Value: Blinking or Off
Port A Bypass State	The state of the Port A Bypass. Possible values include: Bypass Disabled, Bypassed By Disk, Bypassed By User, Bypassed By EMU.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Port A World Wide Name	A unique, 64-bit number assigned to enclosure Port A.
Port B Bypass State	The state of the Port B Bypass. Possible values include: Bypass Disabled, Bypassed By Disk, Bypassed By User, Bypassed By EMU.
Port B World Wide Name	A unique, 64-bit number assigned to enclosure Port B.
Serial Number	The serial number of the component assigned to it by the supplier of the component.
World Wide Name	A unique, 64-bit number assigned to hardware ports.

Logical

Active Path	The path that is currently accessing the disk. Values: Primary, Backup, Mirror, Mirror Backup
Backup Path State	The current state of the backup disk path. Values .
Logical Device Number	The logical device number used by the operating system to identify the disk. Example: 7
Media Size	The total size (in kilobytes) of disk storage space.
Primary Path State	The current state of the primary disk path. Values .
Product ID	A unique number that identifies the product.

Process Pair

Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285
Configured Processors	The two processors in which this I/O process is configured to run. Example: 0,1

Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296

Disk Pair

Disk Pair Name	The name and location of the mirrored disk. Example: Disk \$DATA00-M (1.1.2).
----------------	---

Primary Path

Access State	Indicates whether the primary disk path is active or inactive.
Configured FSAC Location	Displays the configured location of the FCSA FSAC containing the primary disk path controller. This attribute is displayed even if the physical FCSA FSAC is not present. Example: FCSA.SAC-1.GRP-111.MOD-2.SLOT-2
FSAC	Identifies the primary FCSA that manages the disk. Example: FCSA FSAC (111.2.2.1)

Backup Path

Access State	Indicates whether the backup disk path is active or inactive.
Configured FSAC Location	Displays the configured location of the FCSA FSAC containing the backup disk path controller. This attribute is displayed even if the physical FCSA FSAC is not present. Example: FCSA.SAC-1.GRP-111.MOD-3.SLOT-2
FSAC	Identifies the backup FCSA that manages the disk. Example: FCSA FSAC (111.3.2.1)

Firmware

OEM Product ID	The firmware product ID assigned by the supplier.
Version	The version of the firmware running on the disk.

Actions

Abort Backup Path

Terminates operation of the backup path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Backup Path action before you can start the path again.

Abort Disk

Terminates operation of all paths for the disk. When the Abort action finishes, the paths are in a Hard Down state. You must use the Reset Disk action before you can start the paths again.

Abort Primary Path

Terminates operation of the primary path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Primary Path action before you can start the path again.

Blink LED Off

Turns off the blinking of the disk drive's (amber) fault LED.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED OFF

Blink LED On

Causes the disk drive's (amber) fault LED to start blinking.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED ON

Clear Data

Erases all data on the disk but leaves the disk label intact. Clear Data does not erase the FIR data in the CE sector, the volume label, the boot sector, or the spare tracks table. After a Clear Data completes or is cancelled, the disk drive is not usable until you restore the file system by using the SCF INITIALIZE DISK command.

The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

Disable Drive Bypass

Opens up the specified port or ports (A and/or B) on the disk drive for use.

Enable Drive Bypass

Shuts down the specified port or ports (A and/or B) on the disk drive.

Firmware Update

Updates firmware for the Fibre Channel disk drive. This action can be performed only when both Primary and Backup paths are in the Down state.

Replace

Displays the procedure for replacing the disk.

Reset Backup Path

Places the backup path in a state from which it can be started.

Reset Disk

Places the disk in a state from which it can be started. This action might be necessary before starting a disk that has both paths in a Hard Down state; for example, if a hardware error has occurred, if the disk was stopped with an Abort action, or if a Stop or Abort fails to put the disk into the Down state.

If only one disk path is in a Hard Down state, you can use the [Reset Primary Path](#) or [Reset Backup Path](#) as appropriate.

Reset Primary Path

Places the primary path in a state from which it can be started.

Reset Volume

Places the volume in a state from which it can be started.

Responsive Test

Verifies that the disk drive is installed and responding.

Save as System Load Configuration

Specifies, within OSM, this disk as an alternate system load volume. For NonStop BladeSystem NB54000c and NB56000c only, if the action passes and a valid core license file is present in \$SYSTEM, OSM offers to copy the license file copied to each new alternate system disk.

You can specify up to four such alternate system load configurations. Each one is displayed under the system attributes in the OSM Service Connection and can be selected from within the System Load dialog box in the OSM Low-Level Link.

NOTE: With OSM Low-Level Link T0633 AAQ and later, you can also save system configuration files on the system console. Those saved configurations are not displayed as attributes values in the OSM Service Connection, but can be used during the system load operations in the Low-Level Link. For more information, see the OSM Low-Level Link online help.

Spin Down

Stops the physical spinning of the disk drive. This should be done before removing a disk drive. Both paths must be down for the action to succeed.

Spin Up

Starts the physical spinning of the disk drive.

Start Backup Path

Starts the backup path to this disk drive. When the Start action completes, the backup path is in the Started state.

This action fails if both paths to this disk are down and the mirrored disk is Up. For more information, see [Start Disk](#).

Start Disk

Use this action to start all paths to the disk drive only when:

- The disk paths are in a Down state. (Hard Down states require a reset action, either [Reset Disk](#), [Reset Primary Path](#), or [Reset Backup Path](#) as appropriate.)
- Its mirrored disk is not currently Up. The Start Disk action is designed to fail if the mirrored disk is already in an Up state because the mirror and primary disk volumes can have different data and require a revive operation. To revive and bring up the disks properly, use the OSM [Start Volume](#) action or SCF START DISK command.

When the action completes successfully, all paths to the disk are in the Started state.

Start Primary Path

Starts the primary path to this disk drive. When the Start action completes, the primary path is in the Started state.

This action fails if both paths to this disk are down and the mirrored disk is Up. For more information, see [Start Disk](#).

Start Volume

Starts all paths for both the primary and mirror drives of this volume unless they are in a Hard Down state. Disk paths in a Hard Down state require a reset action first (either [Reset Disk](#), [Reset Primary Path](#), or [Reset Backup Path](#) as appropriate).

Stop Backup Path

Terminates the backup path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Disk

Terminates all paths for this disk drive. When the Stop action finishes, the paths are in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Primary Path

Terminates the primary path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Volume

Terminates all paths for the primary and mirror drives of this volume. When the Stop action finishes, the paths are in a Down state.

Switch Process Pair

Switches the primary and backup disk I/O processes.

Switch to Backup Path

Switches processing from the primary to the backup path.

Switch to Primary Path

Switches processing from the backup to the primary path.

Verify Physical Connectivity

Verifies connectivity to the disk on a particular path.

Disk (SAS)

A physical representation of each SAS disk in a [SAS Disk Enclosure](#). A logical representation of each CLIM-attached SAS disk is displayed under the [CLIM-attached Disks](#) object.

System > SAS Disk Enclosures > SAS Disk Enclosure > Disk

Attributes

Physical

Device State	The state of the component as known to the operating system on the server. Values
Media Type	Identifies the media type of the SAS disk drive as either "Magnetic" or "Solid State."
Model	The model number of the SAS disk drive that was assigned in manufacturing.
Serial Number	The serial number of the SAS disk drive.

Firmware

Version	The version of the firmware running on the SAS disk drive.
---------	--

Actions

Firmware Update

Updates the firmware running on the SAS disk drive.

Get Logical Disk(s)

Retrieves the names of the logical disks configured for the physical disk in the SAS disk enclosure.

Replace

Launches a documented service procedure to replace a disk drive in a SAS disk enclosure.

Set LED State

Sets the LED on the physical disk in the SAS disk enclosure to On or Off.

Show SMARTSSD Wear Gauge

This action is available for Solid State drives only. It displays the current SMARTSSD Wear Gauge values, which includes estimates for both the amount of life used up for the disk and for the amount of life remaining. A disk with a low percentage of life used can display an unusually high number of hours of life remaining.

The [Get SMARTSSD Wear Status Summary](#) guided procedure on the System object allows you to display the same information for multiple (any or all selected) drives in a single interface and to save the resulting data in .csv (or comma delimited) format for use in Microsoft Excel.

Start Disk

Starts all partitioned and non-partitioned paths to this disk drive.

Start Volume

Starts all partitioned and non-partitioned paths for both the primary and mirror drives of this volume.

Stop Disk

Stops all partitioned and non-partitioned paths to this disk drive.

DVD-ROM (Blade Element)

In the OSM Service Connection, an object displayed as a subcomponent under the [Blade Element](#) object for Integrity NonStop NS1000, NS1200, NS5000, and NS3000AC servers only.

Attributes

DVD-ROM

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
-------------	---

Actions

None

E4SA (Ethernet 4 ServerNet Adapter)

An adapter that connects the ServerNet connections inside a server to an Ethernet local area network (LAN). The Ethernet 4 ServerNet Adapter (E4SA) CRU contains two Ethernet ServerNet addressable controllers (SACs), each of which contains two Ethernet physical interfaces, for a total of four Ethernet ports on each E4SA CRU.

This Nonstop S-series component can be connected to a Nonstop NS-series system through an IOMF2 enclosure.

Location in OSM Tree: System > Group > Module > E4SA

Slot Location: E4SA CRUs can be located in slots 51, 52, 53, and 54 in IOMF2 enclosures (service side).

Example: E4SA \$ZZLAN.E4SA0 (1.1.53)

Attributes

E4SA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indication of whether the component is powered On or Off.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Disabled ServerNet Ports	Which, if any, ServerNet router ports on this CRU are disabled. OSM actions to disable or enable a ServerNet port are performed as directed by OSM alarm repair actions.
Configured Type	The configuration type of this resource. Value: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the Ethernet 4 ServerNet Adapter (E4SA) CRU and the associated Ethernet ServerNet addressable controller (ESAC). When the Abort action finishes, the E4SA CRU and the ESAC are in the Stopped state.

Disable ServerNet Port

Disables the specified ServerNet router port on this CRU. Perform this action only as directed by OSM alarm repair actions.

Parameter: Port Number

Enable ServerNet Port

Enables the specified ServerNet router port on this CRU. Perform this action only as directed by OSM alarm repair actions.

Parameter: Port Number

Start

Starts the Ethernet 4 ServerNet Adapter (E4SA) CRU and the associated Ethernet ServerNet addressable controller (ESAC). The E4SA CRU and the ESAC must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the ESAC. When the Start action completes, both the E4SA CRU and the ESAC are in the Started state.

Stop

Rather than automatically stopping the E4SA (as the Abort action does), this action first warns you if the E4SA is currently in use (and stops it only after you confirm).

EMU

The Environmental Monitoring Unit (EMU) is a subcomponent of a [FCDM](#).

Location in OSM Tree: System > Group > FCDM Collection > FCDM > EMU

Example: EMU (111.211.1.99)

Attributes

EMU

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Type	The vendor hardware type.
------	---------------------------

Logical

Device State	The state of the component as known to the operating system on the server. Values
Vendor Hardware Revision	A code that identifies the generation of the component provided by its supplier.

Firmware

Version	The version of the firmware configuration currently loaded on the EMU.
---------	--

Actions

Firmware Update

Updates the firmware on the EMU.

Replace

Displays the procedure for replacing the EMU.

Enclosure

The Enclosure object is displayed in the OSM Service Connection (J-series only) to represent a HP BladeSystem c-Class Enclosure in an HP Integrity NonStop BladeSystem. There can be one or two enclosures in each NonStop BladeSystem.

Location in OSM Tree: System > Enclosure

Each Enclosure object contains these subcomponents:

- [Processor Blades](#)
- [Logical Processors](#)
- [ServerNet Switches](#)

Attributes

Enclosure

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Enclosure Name	The name of the Blade enclosure, as configured through the Onboard Administrator (OA). (This name cannot be changed through OSM.)
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component.
Product Name	The product name of the component.
Replacement Part Number	The replacement part number of the component.
Serial Number	The serial number of the component assigned to it by the supplier of the component.

Physical Location

The values displayed by these attributes can be assigned through the [Set Physical Location](#) action, except for the Rack Name.

Rack Name	The Rack Name assigned in the OA and cannot be changed through the OSM Set Physical Location action.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the enclosure within the rack.
Locator	An optional text string assigned to further identify the physical location of the enclosure. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only.

Logical

Active OA IPv4 Address	The IPv4 address of the active OA (Onboard Administrator).
Active OA Status	The status of the active OA (Onboard Administrator), as known by OSM Possible Values: OK, Other, Degraded, Stressed, Predictive Failure, Error, Non-Recoverable Error, Starting, Stopping, Stopped, In Service, No Contact, Lost Communication, Aborted, Dormant, Supporting Entity In Error, Completed, Power Mode, DMTF Reserved, Vendor Reserved, Unknown.

Aggregate Status	This represents the status of the c7000 enclosure, as seen by the OA. Possible Values: Unknown, Other, OK, Degraded, Stressed, Predictive Failure, Error, Non-Recoverable Error, Starting, Stopping, Stopped, In Service, No Contact, Lost Communication, Aborted, Dormant, Supporting Entity In Error, Completed, Power Mode, DMTF Reserved, Vendor Reserved.
Bay 1 OA Firmware Version	The firmware version currently running on the OA (Onboard Administrator) located in Bay 1 of the enclosure; for example: 2.52. NOTE: When looking at the enclosure from the rear, the bay on the left is bay 1, the bay on the right is bay 2.
Bay 2 OA Firmware Version	The firmware version currently running on the OA (Onboard Administrator) located in Bay 2 of the enclosure; for example: 2.52.
Standby OA IPv4 Address	The IPv4 address of the standby OA.
Standby OA Status	The status of the standby OA (Onboard Administrator), as known by OSM Possible Values: OK, Other, Degraded, Stressed, Predictive Failure, Error, Non-Recoverable Error, Starting, Stopping, Stopped, In Service, No Contact, Lost Communication, Aborted, Dormant, Supporting Entity In Error, Completed, Power Mode, DMTF Reserved, Vendor Reserved, Unknown.

Configuration

Power Source A Configuration	Indicates the state of this power supply's power rail as known to OSM. Values: Not Configured, AC, UPS, Unknown You must use the Configure Power Source as UPS action to set either the A or B value to UPS in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS.
Power Source B Configuration	Indicates the state of this power supply's power rail as known to OSM. Values: Not Configured, AC, UPS, Unknown You must use the Configure Power Source as UPS action to set either the A or B value to UPS in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS.
Power Source A UPS IPv4 Address or Power Source B UPS IPv4 Address	Additional attributes displayed only when Power Source A or Power Source B has been configured as UPS, these attributes display the IPv4 address of the UPS that has been configured.

Actions

Configure a Power Source as AC

You must be logged on as super.super to perform this action.

Configure a Power Source as UPS

Allows you to configure the Power Source A or B to use a UPS in a power-fail scenario. Sets the specified [Configuration](#) attribute to UPS. You must be logged on as super.super to perform this action. Upon initiating the action, you are prompted to enter the IPv4 address of the UPS.

You must use this action to configure at least one of your Integrity NonStop BladeSystem power supplies (to specify UPS as the backup power source) in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your UPS. For more information on preparing for AC power-fail scenarios, see the *Integrity NonStop BladeSystems Planning Guide*. For more information on using the POWERFAIL_DELAY_TIME command to specify the Power-Failure-to-Shutdown time interval, see the *SCF Reference Manual for the Kernel Subsystem*.

Delete the Power Source Configuration

Deletes a previously configured Configured AC or UPS backup power source and sets the specified [Configuration](#) attribute value to Not Configured. You must be logged on as super.super to perform this action.

Display Diagnostic Status Errors

Displays all diagnostic status errors for the Enclosure.

Launch the Onboard Administrator

Launches the Onboard Administrator (OA) management page.

Prepare Enclosure for Removal

Prepares the enclosure for removal. This action is not valid for group 100.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the enclosure, with the exception of Rack Name:

- Rack Name – for the enclosure, the rack name is assigned in the OA and cannot be changed through this OSM action.
- Rack Offset is a numerical value representing the location of the enclosure within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action fails.
- Locator is an optional text string to help identify the physical location of the enclosure. It must contain alphanumeric characters only.
- This parameter is used for DC-powered Telco systems only.

You can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system while you create a physical view of your modular racks.

ESS Disk

Enterprise Storage System disk drive. ESS disks are visible in the tree pane and in the Inventory view of the Management window. In the tree pane, expand the ESS Disk Collection object to see the individual ESS disk drives. In the Inventory view, each ESS disk drive is listed on a separate line. ESS disk drives are not visible in the Physical view.

ESS disks connect to your system through FCSAs in [I/O Adapter Module](#) enclosures. For more information, see the *NonStop Hardware Installation Guide* for your system and the *Fibre Channel ServerNet Adapter Installation and Support Guide*.

Location in OSM Tree: System > ESS Disk Collection > ESS Disk

Example: ESS Disk \$DAVON

Attributes

ESS Disk

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Logical Device Number	The logical device number used by the operating system to identify the disk. Example: 7
Backup Path State	The current state of the backup disk path. Values.
Media Size	The total size (in kilobytes) of disk storage space.
Active Path	The path that is currently accessing the disk. Values: Primary, Backup, Mirror, Mirror Backup
Primary Path State	The current state of the primary disk path. Values.

Backup Path

Configured FSAC Location	Displays the configured location of the FCSA FSAC containing the backup disk path SCSI controller. This attribute is displayed even if the physical FCSA FSAC is not present.
Access State	Indicates whether the disk is active or inactive.
LUN	The logical unit number of the disk. Example: 0
FSAC	Represents the actual presence of the FCSA FSAC containing the backup disk path SCSI controller. This attribute is displayed only if the physical FCSA FSAC is present.
Port Name	A number that uniquely identifies the port through which the disk is connected.

Primary Path

Configured FSAC Location	Displays the configured location of the FCSA FSAC containing the primary disk path SCSI controller. This attribute is displayed even if the physical FCSA FSAC is not present.
Access State	Indicates whether the disk is active or inactive.
LUN	The logical unit number of the disk. Example: 0
FSAC	Represents the actual presence of the FCSA FSAC containing the primary disk path SCSI controller. This attribute is displayed only if the physical FCSA FSAC is present.
Port Name	A number that uniquely identifies the port through which the disk is connected.

Disk Pair

Disk Pair Name	The name of the ESS disk that this disk is paired with. A "-P" designation following the disk name indicates primary disk. "-M" indicates mirrored disk.
----------------	--

Process Pair

Configured Processors	The 2 processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296

Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285

Actions

Abort Backup Path

Terminates operation of the backup path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Backup Path action before you can start the path again.

Abort Disk

Terminates operation of all paths for the disk. When the Abort action finishes, the paths are in a Hard Down state. You must use the Reset Disk action before you can start the paths again.

Abort Primary Path

Terminates operation of the primary path to the disk. When the Abort action finishes, the path is in the Stopped state.

Reset Backup Path

Places the backup path in a state from which it can be started.

Reset Disk

Places the disk in a state from which it can be started. This action might be necessary if the disk was in a STOPPED state, substate HARDDOWN; a hardware error has occurred; the disk was stopped with an ABORT command; or a STOP or ABORT fails to put the disk into the STOPPED state, substate DOWN.

Reset Primary Path

Places the primary path in a state from which it can be started.

Reset Volume

Places the volume in a state from which it can be started.

Responsive Test

Verifies that the disk drive is installed and responding.

Start Backup Path

Starts the backup path to this disk drive. When the Start action completes, the backup path is in the started State.

Start Disk

Starts all paths to this disk drive. When the Start action completes, all paths are in the Started state.

Start Primary Path

Starts the primary path to this disk drive. When the Start action completes, the primary path is in the Started state.

Start Volume

Starts all paths for both the primary and mirror drives of this volume.

Stop Backup Path

Terminates operation of the backup path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Disk

Terminates all paths for this disk drive. When the Stop action finishes, the paths are in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Primary Path

Terminates the primary path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Volume

Terminates all paths for the primary and mirror drives of this volume. When the Stop action finishes, the paths are in a Down state.

Switch Process Pair

Switches the primary and backup disk I/O processes.

Switch to Backup Path

Switches processing from the primary to the backup path.

Switch to Primary Path

Switches processing from the backup to the primary path.

ESS Disk Collection

Contains all [ESS Disks](#) that are connected to the system.

Location in OSM Tree: Under System

Example: ESS Disk Collection

Attributes

None.

External Disk

An external disk drive that connects to a system through the [ServerNet/DA](#) CRU. The External Disk CRU is housed in an 8-slot disk enclosure that is physically connected to a [Fiber SAC](#) (ServerNet addressable controller) mounted on the ServerNet/DA CRU.

External disks are visible in the tree pane and in the Inventory view of the Management window. In the tree pane, expand the External Disk Collection to see the individual external disk drives. In the Inventory view, each external disk drive is listed on a separate line. External disk drives are not visible in the Physical view.

Location in OSM Tree: System > External Disk Collection > External Disk

Slot Location: External to enclosures

Example: External Disk \$MARS2-P

Attributes

External Disk

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Logical

Logical Device Number	The logical device number used by the operating system to identify the disk. Example: 7
Backup Path State	The current state of the backup disk path. Values
Media Size	The total size (in kilobytes) of disk storage space.
Primary Path State	The current state of the primary disk path. Values
Product ID	A unique number that identifies the product.
Active Path	The path that is currently accessing the disk. Values: Primary, Backup

Process Pair

Configured Processors	The 2 processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296
Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285

Disk Pair

Disk Pair Name	The name of the disk paired with this one. Example: External Disk \$KLAM2-M
----------------	---

Backup Path

SCSI ID	An identification number assigned to the device when configured.
SCSI Controller	A number (1 or 2) that identifies the backup SCSI controller that manages the disk. Example: SCSI Controller (1.1.50.2)
Access State	The accessibility of the backup path. Values: Inactive, Active
Configured Controller Location	The location of the backup disk path SCSI controller. Example: IOMF2.SAC-2.GRP-1.MOD-1.SLOT-55

Primary Path

SCSI ID	An identification number assigned to the device when configured.
SCSI Controller	A number (1 or 2) that identifies the primary SCSI controller that manages the disk. Example: SCSI Controller (1.1.50.2)
Access State	The accessibility of the primary path. Values: Inactive, Active
Configured Controller Location	The location of the primary disk path SCSI controller. Example: IOMF2.SAC-2.GRP-1.MOD-1.SLOT-50

Firmware

Version	The version of the firmware running on the disk.
---------	--

Actions

Abort Backup Path

Terminates operation of the backup path to the disk. When the Abort action finishes, the path is in a Hard Down state. You must use the Reset Backup Path action before you can start the path again.

Abort Disk

Terminates operation of all paths for the disk. When the Abort action finishes, the paths are in a Hard Down state. You must use the Reset Disk action before you can start the paths again.

Abort Primary Path

Terminates operation of the primary path to the disk. When the Abort action finishes, the path is in the Stopped state.

BLINK LED Off

Stops the blinking of the fault LED initiated by the Blink LED On action.

BLINK LED On

Causes the fault LED to blink to make it easier to identify the component.

Clear Data

Erases all data on the disk but leaves the disk label intact. Clear Data does not erase the FIR data in the CE sector, the volume label, the boot sector, or the spare tracks table. After a Clear Data

action completes or is cancelled, the disk drive is not usable until you restore the file system by using the SCF Alter Label command.

The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

Firmware Update

Updates disk drive firmware.

Reset Backup Path

Places the backup path in a state from which it can be started.

Reset Disk

Places the disk in a state from which it can be started. This action might be necessary if the disk was in a STOPPED state, substate HARDDOWN; a hardware error has occurred; the disk was stopped with an ABORT command; or a STOP or ABORT fails to put the disk into the STOPPED state, substate DOWN.

Reset Primary Path

Places the primary path in a state from which it can be started.

Reset Volume

Places the volume in a state from which it can be started.

Responsive Test

Verifies that the disk drive is installed and responding.

Start Backup Path

Starts the backup path to this disk drive. When the Start action completes, the backup path is in the started State.

Start Disk

Starts all paths to this disk drive. When the Start action completes, all paths are in the Started state.

Start Primary Path

Starts the primary path to this disk drive. When the Start action completes, the primary path is in the Started state.

Start Volume

Starts all paths for both the primary and mirror drives of this volume.

Stop Backup Path

Terminates operation of the backup path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Disk

Terminates all paths for this disk drive. When the Stop action finishes, the paths are in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Primary Path

Terminates the primary path to the disk. When the Stop action finishes, the path is in a Down state. If the disk drive is currently in use, a dialog box warns you and asks whether or not you want to continue with the action.

Stop Volume

Terminates all paths for the primary and mirror drives of this volume. When the Stop action finishes, the paths are in a Down state.

Switch to Backup Path

Switches processing from the primary to the backup path.

Switch to Primary Path

Switches processing from the backup to the primary path.

Test Verify

Runs the power-on self-test for the disk and tests the internal circuitry of the drive.

Validate Checksum

Scans the user data area of a disk for sector checksum errors. If the action fails, the Action Details dialog box reports a sector checksum error and suggests that you spare the sector only if you believe there is a drive media problem.

For additional information, use the OSM Event Viewer. Retrieve events using \$ZLOG as the source criteria and RAL as the subsystem criteria, and look for Disk-sector-failure events (event number 7001). In the event detail, a Sector-failure-count token shows how many sector checksum errors were found, and a Disk-logical-sector token appears for each error, providing the logical address of that failing sector.

You can perform the Validate Checksum action while the disk drive is in use. The action prompts you to specify an optional process priority for the action. If not specified, the current default priority is used.

External Disk Collection

When one or more external disks are connected to a system, an External Disk Collection object appears in both the tree pane and the overview pane of the OSM Service Connection. In both panes, this object displays an alarm or yellow icon if alarms or degraded conditions exist on any of the individual external disks contained within. You can expand the External Disk Collection icon in the tree pane (but not in the overview pane) to select and monitor individual external disks.

Location in OSM Tree: Under System

Example: External Disk Collection

Attributes

None.

Actions

None.

Fan

A component that circulates air into the enclosure to help maintain optimal temperature. Each system enclosure contains two fans.

Location in OSM Tree: System > Group > Module > Fan

Example: Fan (1.1.22)

Attributes

Fan

Service State	Displayed in the Attributes tab and Attributes dialog box only if attention or service is required. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Power State	Whether the component is powered on. Values

Logical

Enabled State	The current state of the fan as known to the operating system. Values
---------------	---

Rotations Sensor

Normal Minimum Value	The minimum acceptable fan speed is 1800 RPM. If the speed falls below 1800, an alarm is generated.
Current Value	The current fan speed, measured in rotations per minute (RPM). Alarms are generated if the speed of the fan falls below 1800 (minimum RPM) or rises above 5800 (maximum RPM).
Normal Maximum Value	The maximum acceptable fan speed is 5800 RPM. If the speed rises above 5800, an alarm is generated.

Actions

Enable/Disable

Restores or stops power to the fan. After servicing the fan or its associated PMCU, perform the Enable action.

Parameter: Enabled (true = enabled, false = disabled)

Fan Assembly (Blade Element)

In the OSM Service Connection, Fan Assembly objects are displayed as subcomponents under the [Blade Element](#) object for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC servers only.

Attributes

Fan Assembly

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. NOTE: Not displayed for NS2100, NS2200 series, NS2300, or NS2400 series.
-------------	--

Logical

Device State	The state of the fan as reported by OSM. Possible values include OK,FAN_CRITICAL_FAULT, etc.
--------------	--

Actions

None

Fan (CLIM)

A subcomponent of the [CLIM](#).

Location in OSM Tree: System > CLIMs > CLIM > Fan

Attributes

Fan

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the fan as reported by OSM. Possible values include: OK, Degraded, Fault, Not Installed.
--------------	---

Actions

Replace

Launches a documented service procedure to replace a fan in a CLIM.

Fan (IOAM)

An [IOAM](#) component that circulates air into the enclosure to help maintain optimal temperature. There are two fans in each IOAM, for a total of four in each IO enclosure.

NOTE: If a ServerNet switch board is not present, the IOAM fans will not appear in OSM.

For information on how to replace an individual IOAM Fan, see *Replacing a Fan in an IOAM Enclosure* in the Support and Service > Service Procedures > IOAM Hardware Servicing collection in NTL.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > Fan

Example: Fan (13.2.16)

Attributes

Physical

LED State	Indicates whether or not the fan's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
-----------	---

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Set LED State

Turns on or off the amber LED located on the fan. The current state is indicated by the [LED State](#) attribute.

Fan (Processor Switch)

One of two FRUs that provide cooling for the components in a processor switch.

Location in OSM Tree: System > Fabric Group > Internal ServerNet Fabric > Processor Switch > Fan

Example: Fan (100.2.16)

Attributes

Physical

LED State	Indicates whether or not the power supply's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
-----------	--

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Replace

Displays the guided procedure to replace a processor switch fan.

Set LED State

Turns on or off the amber LED located on the PIC port. The current state is indicated by the [LED State](#) attribute.

Fan (SAS Disk Enclosure)

A subcomponent of a [SAS Disk Enclosure](#).

System > SAS Disk Enclosures > SAS Disk Enclosure > Fan

Attributes

None.

Actions

Replace

Launches a documented service procedure to replace a fan in a SAS disk enclosure.

Fan (VIO)

A component of VIO enclosures (represented in the OSM Service Connection as [VIO modules](#)) that circulates air into the enclosure to help maintain optimal temperature. There are two fans in each VIO enclosure.

Attributes

Physical

LED State	Indicates whether or not the fan's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Manufacturer	Identifies the manufacturer of the component. Displayed for VIO fans in S-series VIO modules only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Replace

Displays a service procedure describing how to replace a fan in a VIO enclosure.

Set LED State

Turns on or off the amber LED located on the fan. The current state is indicated by the [LED State](#) attribute.

FC Card (CLIM)

A subcomponent of the [CLIM](#).

Location in OSM Tree: System > CLIMs > CLIM > FC Card

Attributes

Physical

Model	The product name of the FC card.
Serial Number	The serial number of the FC card.

Logical

Device State	The state of the FC Card as known to the operating system on the server. Possible values include: OK, Degraded, Fault, Power Off.
Node WWN	The World Wide Name (WWN) assigned to the node.
Port WWN	The World Wide Name (WWN) assigned to the port.

BIOS

Compare State	Indication of the differences, if any, between the current and default BIOS versions. Values
Default File Name	The name of the file to be used for a BIOS update.
Default File Version	The version of the firmware to be used for a BIOS update.
Version	The version of the BIOS running on the FC card.

Firmware

Compare State	Indication of the differences, if any, between the current and default firmware versions. Values
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Version	The version of the firmware running on the FC card.

Actions

BIOS Update

Updates the BIOS running on the FC card.

Firmware Update

Updates the firmware running on the FC card.

Replace

Launches a documented service procedure to replace an FC card in a CLIM.

FC-AL I/O Module

Subcomponent of a [FCDM](#).

There are two FC-AL I/O modules in each FCDM. These modules are the interface between the FCDM elements and the host controller. They route data to and from the drives using loop A and loop B.

Location in OSM Tree: System > Group > FCDM Collection > FCDM > FC-AL I/O Module

Example: FC-AL I/O Module (111.211.1.93)

Attributes

FC-AL I/O Module

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

LED State	Indicates whether or not the FC-AL I/O Module's (amber) fault LED is blinking. Value: Blinking or Off
Type	The vendor hardware type.

Logical

Device State	The state of the component as known to the operating system on the server. Values
Vendor Hardware Revision	A code that identifies the generation of the component provided by its supplier.

Device Connection

Configured Controller Location	The location of the configured FCSA connected to the FC-AL I/O Module. Example: FCSA.FSAC-1.GRP-111.MOD-2.SLOT-1
Fibre Channel Controller	The number that identifies the FCSA FSAC connected to the FC-AL I/O Module. Example: FCSA FSAC (111.2.1.1)

Actions

Blink LED Off

Turns off the blinking of the FC-AL I/O Module's (amber) fault LED.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED OFF

Blink LED On

Causes the FC-AL I/O Module's (amber) fault LED to blink on and off.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED ON

Replace

Displays the procedure for replacing the FC-AL I/O module.

FCDM

Fibre Channel disk modules (FCDMs), formerly known as Disk Drive Enclosures, are located in the OSM Service Connection tree pane hierarchy under FCDM Collection objects. (See [FCDM Collection](#) for more information on where they appear in the tree hierarchy.) Each FCDM contains:

- Up to 14 [Fibre Channel disk drives](#)
- Two [FC-AL I/O Modules](#)
- Two [Power Supplies](#)
- Two [Blowers](#)
- One [EMU](#)

Location in OSM Tree: System > Group > FCDM Collection > FCDM

Example: FCDM (111.211.1)

Attributes

FCDM

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Serial Number	The serial number of the component assigned to it by the supplier of the component.
Type	The vendor hardware type.

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the FCDM is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the FCDM within the rack.
Locator	An optional text string assigned to further identify the physical location of the FCDM. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical Location action. This attribute is displayed only if a value is specified through the action.

Logical

Vendor Product ID	The product identifier of the component assigned to it by the supplier of the component.
Vendor Product Revision	A code that identifies the generation of the component. Assigned by the supplier of the component.
World Wide Name	A unique, 64-bit number assigned to the hardware ports.

Path B

Configured Controller Location	The location of FCSA connected to the disk drive through Port B. Example: FCSA.FSAC-1.GRP-111.MOD-2.SLOT-1
Fibre Channel Controller	Identifies the FCSA FSAC connected to the FCDM through Port B. Example: FCSA FSAC (111.2.1.1)

Path A

Configured Controller Location	The location of FCSA connected to the disk drive through Port A. Example: FCSA.FSAC-1.GRP-111.MOD-2.SLOT-1
Fibre Channel Controller	Identifies the FCSA FSAC connected to the FCDM through Port A. Example: FCSA FSAC (111.2.1.1)

Actions

Blink All LEDs Off

Turns off the blinking of the fault LEDs on the FCDM, disks, FC-AL I/O module, power supplies, and fans.

Blink All LEDs On

Causes the fault LEDs on the FCDM, disks, FC-AL I/O module, power supplies, and fans to blink.

Disable All Drive Bypass

Opens up the specified port or ports (A and/or B) on all disk drives in the FCDM for use.

Enable All Drive Bypass

Shuts down the specified port or ports (A and/or B) on all disk drives in the FCDM.

Replace

Displays the procedure for replacing the FCDM.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the FCDM:

- Rack Name is a user-defined name for the rack containing the FCDM. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the FCDM within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action fails.
- Locator is an optional text string to help identify the physical location of the FCDM. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. A system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system while you create a physical view of your modular racks.

Verify Path A Access

Verifies that Path A from the FCDM via FC-AL I/O module A to the FCSA FSAC is responding.

Verify Path B Access

Verifies that Path B from the FCDM via FC-AL I/O module B to the FCSA FSAC is responding.

FCDM Collection

The OSM Service Connection displays all [Fibre Channel disk modules \(FCDMs\)](#) within FCDM Collection objects, whether or not they are daisy-chained. FCDMs that are daisy-chained together (up to four) are displayed within the same FCDM Collection object. If an FCDM Collection object contains only one FCDM, it is not daisy-chained. Other FCDMs that are not daisy-chained appear under separate in FCDM Collection objects.

The FCDM Collection object appears within the same group object as the IOAM enclosure to which the FCDM is connected. If the FCDM is connected to Fibre Channel ServerNet adapters located in different IOAM enclosures (for increased fault tolerance), OSM displays the FCDM Collection in the lower-numbered group.

For information on daisy-chaining FCDMs, see the *NonStop NS-Series System Expansion and Reduction Guide*.

Location in OSM Tree: System > Group > FCDM Collection

Example: FCDM Collection (111.211)

Attributes

FCDM Collection

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Path B

Configured Controller Location	The location of FCSA connected to the disk drive through Port B. Example: FCSA.FSAC-1.GRP-111.MOD-2.SLOT-1
Fibre Channel Controller	Identifies the FCSA FSAC connected to the FCDM through Port B. Example: FCSA FSAC (111.2.1.1)

Path A

Configured Controller Location	The location of FCSA connected to the disk drive through Port A. Example: FCSA.FSAC-1.GRP-111.MOD-3.SLOT-1
Fibre Channel Controller	Identifies the FCSA FSAC connected to the FCDM through Port A. Example: FCSA FSAC (111.3.1.1)

Actions

None.

FCSA

Fibre Channel ServerNet adapter. The FCSA object always displays two [FCSA FSACs](#), regardless of whether they are both physically present. At least one must be present to perform FCSA firmware updates. The FCSA FSAC attributes [Node Name](#) and [Port Name](#) indicate the presence of FCSA FSACs and attached disks. Unlike many other adapters, the ports on the FCSA are numbered from top down when viewing the FCSA installed in a rack. Thus, FCSA FSAC 1 is attached to the upper port (port 1) and FCSA FSAC 2 is attached to the lower port (port 2).

NOTE: If a ServerNet switch board is not present, FCSAs do not appear in OSM.

OSM does not display FCSA attribute information until an associated disk process is configured and started. For more information, see the *Fibre Channel ServerNet Adapter Installation and Support Guide*.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > FCSA

Example: FCSA (13.3.1)

Attributes

FCSA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Flash Firmware

Information about the version of the operational firmware located in the Flash memory of the FCSA.

Version	The version of the flash firmware running on the FCSA.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Compare State	Indication of the differences, if any, between the current and default firmware versions. Values

Flash Boot Firmware

Information about the version of the boot firmware located in the Flash memory of the FCSA.

Version	The version of the boot firmware running on the FCSA.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	Indication of the differences, if any, between the current and default firmware versions. Values

Actions

Flash Boot Firmware Update

Updates the boot firmware in Flash memory of the FCSA. It is not possible to do this update unless the FCSA has a disk configured through it. If the Flash Boot Firmware Compare State is Unknown, an update attempt will likely fail.

Flash Firmware Update

Updates the operational firmware in Flash memory of the FCSA.

Replace

Launches an interactive action to assist with replacement of an FCSA.

Note: This replacement procedure is intended for authorized service providers only.

When initiated, OSM checks for any connected paths that do not have a backup and warns you of any connectivity loss that could result from continuing with the action. OSM also directs you to the online help for precautionary guidelines for handling the hardware. See:

- [Removing the FCSA](#)
- [Installing the Replacement FCSA](#)

Once you confirm that the FCSA has been replaced, OSM presents these options for bringing up the paths associated with this adapter:

- Bring up and balance. This option makes the -P (primary) and -M (mirror) paths active.
- Bring up only. This option starts the path only if the other path is already up.
- Leave down.

Responsive Test

Verifies that the FCSA is connected and responding.

Test Verify

Verifies basic functionality of the FCSA.

Removing and Installing a Fibre Channel ServerNet Adapter

Removing the FCSA

NOTE: Whenever you handle a FCSA, follow standard operating practices to avoid damage to the equipment. Review the standard operating practices documented in the *Fibre Channel ServerNet Adapter Installation and Support Guide*.

1. Find the group, module, and slot of the IOAM in which the FCSA is installed.
2. Tag the Fibre Channel cables connected to the FCSA with physical labels, preferably at both cable ends. The labels should include:
 - A description of the equipment and connector to which the cables are to be connected
 - The slot location of the FCSA to which the cable is connected
3. Disconnect the Fibre Channel cables one at a time by squeezing the plastic retaining clip at the end of the cable and gently pulling.
4. Protect the equipment from electrostatic discharge:
 - a. Place an antistatic table mat on a flat horizontal work surface near the IOAM enclosure.
 - b. Put on an ESD wrist strap.
 - c. Attach the grounding clip from the ESD wrist strap to any unpainted metal surface on the IOAM enclosure or on the rack in which the enclosure is installed.

⚠ CAUTION: Do not attach the ESD grounding clip to doors or to any painted surface.

5. Press down on the ejector to unseat the adapter. The adapter must be pulled at least two inches out of its slot to be unseated. If the adapter is not unseated far enough, a long connector pin in the midplane can still be engaged with the FCSA. This will make some software behave as though the FCSA is still in its slot but is broken.
6. Grasp the FCSA by its ejector in one hand and slowly pull the FCSA part way out of the slot.

7. Grasp the FCSA by its handle while supporting the bottom edge of the FCSA with the other hand and pull the FCSA the rest of the way out of the slot.

NOTE: The FCSA weighs approximately 7.25 pounds (3 kilograms).

8. Place the FCSA on the antistatic mat.

Installing the Replacement FCSA

NOTE: Whenever you handle a FCSA, follow standard operating practices to avoid damage to the equipment. Review the standard operating practices documented in the *Fibre Channel ServerNet Adapter Installation and Support Guide*.

1. Unpack and inspect the FCSA:
 - a. Put on an ESD wrist strap and attach the grounding clip to the antistatic mat.
 - b. Place the package containing the FCSA on the antistatic mat.
 - c. Open the packing container and remove the FCSA.

Δ **CAUTION:** When opening the packing container, be careful not to cut into the ESD protective bag.

- d. Visually inspect the FCSA and the backplane connector for damage. Use a flashlight, if necessary, to check for bent or broken pins. If the FCSA is damaged or has a damaged connector-pin socket, do not install it.

Δ **CAUTION:** If you insert a FCSA that has a damaged socket into a slot, that FCSA's backplane pins and the connectors on other adapter boards also inserted into that slot can be damaged. Moving a damaged adapter from slot to slot can damage other slots and other adapters.

2. Disconnect the grounding clip of your ESD wrist strap from the antistatic mat, and then connect it to an unpainted metal surface on the FCSA.

Δ **CAUTION:** Do not attach the ESD grounding clip to doors or to any painted surface.

3. Carry the FCSA to the enclosure:
 - a. Grasp the FCSA by its handle in one hand, while supporting the bottom edge of the FCSA with the other hand.

NOTE: The FCSA weighs approximately 7.25 pounds (3 kilograms).

- b. Carry the FCSA to the back of the IOAM enclosure.
 - c. Set the FCSA down on an antistatic mat right side up with the ejector at the top.
4. Disconnect the grounding clip of your ESD wrist strap from the FCSA and connect it to any unpainted metal surface on the IOAM enclosure or on the rack in which the enclosure is installed.
5. Insert the FCSA:
 - a. Using both hands, hold the FCSA so that its ejector is at the top.
 - b. Insert the adapter into its slot in the enclosure.

- c. Firmly push the FCSA to the rear of its slot, but do not force it.

⚠ CAUTION: To avoid damaging the connector pins, apply equal pressure to both the top and bottom of the FCSA when pushing it into its slot. If you try to push the FCSA into its slot when the pins in either the FCSA or the midplane are damaged, you must replace both the FCSA and the enclosure.

- d. Press down and back on the ejector. The ejector will slide under the top lip of the frame and secure the adapter in place.

6. Disconnect the grounding clip of your ESD wrist strap from the rack or enclosure.

7. Connect the Fibre Channel cables to the Fibre Channel ports on the FCSA by lining up the retaining clips with the ports and gently inserting them into the ports, one at a time.

The green power-on LED at the bottom of the adapter should now be lit. If the LED is not lit, either reseal the FCSA or install a different FCSA.

8. After you install the new FCSA, refer to the *Fibre Channel ServerNet Adapter Installation and Support Guide* for information about resuming operations.

Once you confirm that the FCSA has been replaced, OSM presents these options for bringing up the paths associated with this adapter:

- Bring up and balance. This option makes the -P (primary) and -M (mirror) paths active.
- Bring up only. This option starts the path only if the other path is already up.
- Leave down.

FCSA FSAC

A Fibre Channel SAC (ServerNet addressable controller) is one of two fiber-optic plug-in cards mounted on an **FCSA** (Fibre Channel ServerNet adapter) in an IOAM. In a VIO enclosure, the FCSA FSAC object represents the functional equivalent on a **VIO FCSA**.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > FCSA > FCSA FSAC

or, in a VIO enclosure:

System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > FCSA > FCSA FSAC

Example: FCSA FSAC (100.2.1.1)

NOTE: The ports on a Fibre Channel ServerNet adapter are numbered from top down when you view the FCSA installed in a rack. Thus, FCSA FSAC 1 is attached to the upper port (port 1), FCSA FSAC 2 is attached to the lower port (port 2).

Attributes

FCSA FSAC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
Node Name	A number (read from the hardware) that uniquely identifies each FCSA FSAC. Until an attached disk is configured and started, the Node Name attribute is displayed as 0xFFFFFFFFFFFFFFF.
Port Name	A number (read from the hardware) that uniquely identifies each Fibre Channel port connected to the FCSA FSAC. Until an attached disk is configured and started, the Port Name attribute is displayed as 0xFFFFFFFFFFFFFFF.

Actions

Responsive Test

Verifies that the FCSA FSAC is present and responding. (To pass the test, a disk using this FSAC must be configured and started.)

FESA (Fast Ethernet ServerNet Adapter)

An adapter that connects the ServerNet connections inside a server to a 10/100Base-TX local area network (LAN).

The Fast Ethernet ServerNet adapter (FESA) CRU contains one Fast Ethernet ServerNet addressable controller (SAC), which contains one Ethernet physical interface, that corresponds to the one Ethernet port on each FESA CRU.

Location in OSM Tree: System > Group > Module > FESA

Slot Location: FESA CRUs can be located in slots 51, 52, 53, and 54 in IOMF2 enclosures (service side).

Example: FESA \$ZZLAN.FESA1 (1.1.53)

Attributes

FESA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the Fast Ethernet ServerNet adapter (FESA) and the associated Ethernet ServerNet addressable controller (SAC). When the Abort action finishes, the FESA and the SAC are in the Stopped state.

Start

Starts the Fast Ethernet ServerNet adapter (FESA) and the associated Ethernet ServerNet addressable controller (SAC). The FESA and the SAC must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the SAC. When the Start action completes, both the FESA and the SAC are in the Started state.

Stop

Rather than automatically stopping the FESA (as the Abort action does), this action first warns you if the FESA is currently in use (and stops it only after you confirm).

Fiber

OSM displays four Fiber objects under the [ServerNet Ports](#) on a [ServerNet Switch](#) in blade enclosures.

Location in OSM Tree: System > Enclosure > ServerNet Switch > Port > Fiber.

Attributes

None.

Fiber

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Link Status	The state of the component as known to the operating system on the server. Values
Neighbor Check Status	

Actions

None.

Fibre Channel Router

Allows two SCSI tape devices to be connected to a port on a Fibre Channel ServerNet Adapter (FCSA). After the router is connected to the maintenance LAN and initially configured, as described in the *M8201R Fibre Channel to SCSI Router Installation and User's Guide*, you can use OSM actions [Start Monitoring Fibre Channel Router](#) (located under the Monitored Service LAN Devices object) to have OSM discover and start monitoring the router, and [Link to Web Interface](#) (under the Fibre Channel Router object) to access its browser-based configuration interface.

Location in OSM Tree: System > Monitored Service LAN Devices > Fibre Channel Router

Attributes

Physical

Model	The model of the router. Currently supported option: Fibre Channel to SCSI Router.
MAC Address	The media access control (MAC) address of the router.

World Wide Port Name	The name of the fibre channel port that connects the router to the FCSA.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
DHCP Setting	Indicates whether IP address assignment by DHCP (for this router) is enabled or disabled.
IPv4 Address	The IPv4 address of the router. Currently supported model: M8201.
ROM Version	The version of the ROM on the router.
FC Port Status	Indicates whether the fibre channel port connecting the router to the FCSA is up or down.
Serial Number	A unique identification number assigned to each switch in manufacturing.
Firmware Revision	The version of the firmware running on the router.
Device Status	Indicates whether the router is Up or Down.

Associated Device

Tape Drive	The names of the one or two tape drives associated with the router.
------------	---

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the Fibre Channel Router is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the Fibre Channel Router within the rack.

Actions

Link to Web Interface

Opens a Web interface that provides detailed device configuration and information for the router.

Rediscover

Causes OSM to refresh and reanalyze the object. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Stop Monitoring

Stops OSM from monitoring the router.

FSAC (Fiber ServerNet Addressable Controller)

The Fiber SAC (ServerNet addressable controller) is a fiber-optic plug-in card mounted on the [ServerNet/DA](#) CRU. External storage devices are physically connected to the Fiber SACs. There can be up to four Fiber SACs on each ServerNet/DA CRU.

Location in OSM Tree: System > Group > Module > SNDA > FSAC

Example: FSAC (11.1.53.1)

Attributes

FSAC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Track ID	The track ID of the switch logic board.
Part Number	The part number of the switch logic board.
Hardware Revision	The hardware revision of the switch logic board.
CRU Type	The type of CRU this SAC is connected to. Values: SSAC, FSAC, SCSI

Logical

Configured Type	The type of storage device supported by this Fiber SAC. Values: Disk, Tape, SCSI Controller, Not Configured, Unknown
-----------------	--

Actions

Responsive Test

Verifies that the component is connected and responding.

G4SA

The M8800 Gigabit Ethernet 4-port ServerNet adapter (G4SA) provides Gigabit connectivity between NonStop servers and Ethernet LANs. G4SAs are installed in slots 1 through 5 of an [I/O Adapter Module](#) (IOAM).

Each G4SA contains one [G4SA SAC](#), which contains up to four [G4SA PIFs](#), resulting in four Ethernet ports on each G4SA. For more information about the G4SA, including diagrams to identify specific ports, see the *Gigabit Ethernet 4-Port Adapter Installation and Support Guide*.

NOTE: If a ServerNet switch board is not present, G4SAs will not appear in OSM.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > G4SA

Example: G4SA \$ZZLAN.G4SA1 (13.3.2)

Attributes

G4SA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the G4SA and the associated Ethernet ServerNet addressable controller (SAC). When the Abort action finishes, the G4SA and the SAC are in the Stopped state.

Add

This action is displayed in OSM **only** when a G4SA is first inserted and not yet configured. Performing this action ensures that the [Configured Type](#) is set to G4SA.

Delete

Deconfigures the G4SA, removing the associated G4SA SAC and PIF objects. This action can only be performed after you delete the [LIF](#) associated with each G4SA PIF.

Power Off

Physically powers off the G4SA.

Reset

Places the G4SA in a state from which it can be started.

Start

Starts the G4SA and the associated G4SA SAC. The G4SA and the SAC must be in the Stopped state before you perform this action.

Stop

Rather than automatically stopping the G4SA (as the Abort action does), this action first warns you if the G4SA is currently in use (and stops it only after you confirm).

G4SA PIF

Physical interface (PIF) objects represent each of the four ports on a G4SA through which LAN connections are made.

Each G4SA PIF has an associated [LIF](#) object.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > G4SA > G4SA SAC > G4SA PIF

or, in a VIO enclosure:

System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > G4SA > G4SA SAC > G4SA PIF

Example: G4SA PIF \$ZZLAN.G4SA1.0.A

Attributes

G4SA PIF

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Configured Interface Type	Displays the configured interface, as specified by the Alter Interface Type action. Values: Copper, Fiber, or Autodetect.
Current Configured Speed	The transmission rate for the ServerNet addressable controller.
Device State	The state of the component as known to the operating system on the server. Values
Duplex Mode	The transmission mode for the ServerNet addressable controller. Values: Half Duplex, Full Duplex, Unknown
Hardware MAC Address	The media access control (MAC) address of the PIF hardware.
Interface Type	Displays the actual interface that is physically present. Values: Copper, Fiber, and Unknown (if nothing is plugged in)
Link Pulse State	A value of Up confirms that the cable from the PIF to the LAN is connected and operational. A value of Down indicates a problem with LAN connectivity.
Maximum Speed	The maximum transmission rate for the ServerNet addressable controller. Values: 10 megabits per second, 100 megabits per second, Unknown
Network MAC Address	The media access control (MAC) address of the PIF network.
Processors with Data Path	Lists the processor numbers for processors that have a successful data path to the PIF. If no processor has a path, "None" is shown. Example: 1,2,3,8,9

Actions

Abort

Terminates operation of the G4SA PIF. When the Abort action finishes, the PIF is in the Stopped state.

Alter Interface Type

Allows you to set the [Configured Interface Type](#) to either Autodetect, Copper, or Fiber.

Fiber is a valid option only for PIF C or D. (The action fails if you select Fiber for PIF A or B.)

In most cases, the Autodetect option will work. However, if you have a fiber cable connected to one of the PIF ports and a copper cable to the other, and you want to use the copper cable, you must specify Copper (because autodetect checks for the presence of a fiber cable first).

Configure LIF

Configures the associated LIF.

Start

Starts the G4SA PIF. The PIF must be in the Stopped state before you perform this action. When the Start action completes, the PIF is in the Started state.

Stop

Rather than automatically stopping the G4SA PIF (as the Abort action does), this action first warns you if the PIF is currently in use (and stops it only after you confirm).

G4SA SAC

A ServerNet addressable controller mounted on a [G4SA](#) (Gigabit Ethernet 4-port ServerNet adapter) or the functional equivalent on a [VIO G4SA](#).

Each G4SA SAC contains up to four [G4SA PIFs](#), which correspond to the four Ethernet ports on each G4SA.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > G4SA > G4SA SAC
or, in a VIO enclosure:

System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > G4SA > G4SA SAC

Example: G4SA SAC \$ZZLAN.G4SA1.0

Attributes

G4SA SAC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Automatic Boot State	Indicates whether the SAC boot firmware is automatically reloaded if it terminates abnormally. Enabled: The boot firmware is automatically reloaded. Disabled: The boot firmware is not automatically reloaded. Unknown: Automatic Boot state could not be read.
Automatic Dump State	Indicates whether the SAC will dump information about the reasons the SAC aborts operations. Values, as established through the SCF AUTODUMP command, are: Disabled: Indicates that the SAC will not autodump. Enabled: Indicates that SAC will autodump. Extended: Indicates that additional information is dumped. The size of an extended G4SA dump file is significantly larger. Use this option only at the direction of HP service provider.
Device State	The state of the component as known to the operating system on the server. Values
Download File Name	The file name of the operational firmware running on the SAC.
Download File Version	The version of the operational firmware running on the SAC.
Dump File Name	Displays the default naming convention for dump files. The default value (\$SYSTEM.SYS00.C061D00) can be altered in SCF. The first dump file name ends in 00. Each subsequent dump file automatically receives the next sequential number.

Owning Processor	The processor to which the G4SA SAC is connected.
Processor Access List	The currently available processors that can access the resource. Example: 0,1,4,8,9

Firmware

Version	The version of the boot firmware for the SAC.
Default File Name	The name of the file to be used for a (boot) Firmware Update .
Default File Version	The version of the firmware to be used for a (boot) Firmware Update .
Compare State	The differences, if any, between the current and default boot firmware versions. Values

Actions

Abort

Terminates operation of the G4SA ServerNet addressable controller. When the Abort action finishes, the SAC is in the Stopped state.

Dump

Copies a memory image from a G4SA SAC to a file on the local system. The file will be the last (highest numbered) file of the chain started with the file specified in the [Dump File Name](#) attribute of the SAC.



CAUTION: The SAC and PIFs will be unavailable while the SAC is being dumped.

Firmware Update

Updates the boot firmware for the G4SA SAC.

Responsive Test

Runs an online test that verifies the SAC is integrated with the LAN subsystem, is owned, and is in the Started state.

Start

Loads the controller operational code and starts the ServerNet addressable controller. The SAC must be in the Stopped state before you perform this action. When the Start action completes, the SAC is in the Started state.

Stop

Rather than automatically stopping the G4SA SAC (as the Abort action does), this action first warns you if the SAC is currently in use (and stops it only after you confirm).

Test Verify

Runs the power-on self-test for the SAC.

GESA (Gigabyte Ethernet ServerNet Adapter)

An adapter that connects the ServerNet connections inside a server to an Ethernet local area network (LAN). The Gigabit Ethernet ServerNet adapter is similar to the Fast Ethernet ServerNet adapter but offers enhanced performance.

The Gigabit Ethernet ServerNet Adapter (GESA) CRU contains one Gigabit Ethernet ServerNet addressable controller ([SAC](#)), which contains one Ethernet physical interface ([PIF](#)), resulting in one Ethernet port on each GESA CRU.

Location in OSM Tree: System > Group > Module > GESA

Slot Location: GESA CRUs can be located in slots 51, 52, 53, and 54 in IOMF2 enclosures (service side).

Example: GESA \$ZZLAN.GESA0 (1.1.53)

Attributes

GESA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the Gigabyte Ethernet ServerNet adapter (GESA) and the associated Ethernet ServerNet addressable controller (SAC). When the Abort action finishes, the GESA and the SAC are in the Stopped state.

Start

Starts the Gigabyte Ethernet ServerNet adapter (GESA) and the associated Ethernet ServerNet addressable controller (SAC). The GESA and the SAC must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the SAC. When the Start action completes, both the GESA and the SAC are in the Started state.

Stop

Rather than automatically stopping the GESA (as the Abort action does), this action first warns you if the GESA is currently in use (and stops it only after you confirm).

Group (IOMF2 or VIO)

This type of group object contains either a legacy Nonstop S-series IOMF2 enclosure or, for NS16000CG or NS5000 only, VIO Modules used to provide a Versatile Ethernet ServerNet enclosure with 4 (V4SE) or 8 (V8SE) Gigabit Ethernet ports.

Location in OSM Tree: Under System

Examples: When the group contains a legacy Nonstop S-series IOMF2 enclosure, it has a 2-digit number, such as Group 11-16, 21-26, etc. When the group contains VIO Modules used to provide V4SE or V8SE, it has a 3-digit number, such as Group 111-115, 211-215, etc.

Attributes

Group

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Service LED State	<p>Indication of whether the service LED is on or off.</p> <p>On: An OSM user has turned on the service LED by using the Set Service LED State action.</p> <p>Off: An OSM user has turned off the service LED by using the Set Service LED State action.</p> <p>Turning on the group service LED helps you locate the group for servicing. This feature is useful when a system consists of multiple enclosures.</p> <p>NOTE: This attribute is not displayed for a Group containing VIO Modules for V4SE or V8SE.</p>
-------------------	---

Actions

Power Off

Upon initiating the action, it first performs precautionary checks to ensure that you can safely power off. These checks ensure that:

- If the group is an enclosure on the inner tetrahedral ring, there are no enclosures off this enclosure.
- There are no IOMF enclosures off this enclosure.

NOTE: This action is not valid for a Group containing VIO Modules for V4SE or V8SE.

If the checks complete successfully, or you choose to disregard any warnings and proceed, the action allows you to disable the batteries and halt the processors.

After these operations complete successfully (or you choose to disregard any warnings), you can complete the action and power off the group.

Set Service LED State

Turns the service light-emitting diode (LED) on or off for this group. Use this action to mark an enclosure to make it easily locatable for service.

Parameter: Service LED State

on: turns LED on

off: turns LED off

NOTE: This action is not valid for a Group containing VIO Modules for V4SE or V8SE.

Group (IOAM, Fabric, G16SE)

Depending on system type and configuration, this Group object may be displayed in OSM to represent:

- IOAM Group
- Fabric Group
- G16SE Group

IOAM Group

An IOAM Group contains an [I/O Adapter Module enclosure](#) and [FCDM Collection](#) objects, which contain Fibre Channel disk modules (FCDMs) that are connected to this IOAM enclosure. If an FCDM is connected to FCSAs located in different IOAM enclosures (for increased fault tolerance), OSM displays the FCDM Collection in the lower-numbered group.

For an HP Integrity NonStop NS16000 series server, numbering of IOAM groups starts at 110. For an HP Integrity NonStop NS14000 or NS1000 server with an IOAM enclosure, that enclosure is located in Fabric Group 100. For other types of NonStop NS-series systems, there are no IOAM enclosures.

For HP Integrity NonStop Bladesystems, possible IOAM groups include Groups 110-115.

Fabric Group

A Fabric Group contains:

- For Integrity NonStop NS5000 or NS16000 series servers, the components that make up both X and Y internal ServerNet fabrics, including a [processor switch](#) and its subcomponents.
- For Integrity NonStop NS14000, NS1000, NS1200, and NS3000AC servers, the internal ServerNet fabric objects, either an [IOAM enclosure](#) (at the top level) or a [VIO module](#) (within each internal ServerNet fabric object), and any [FCDMs](#) connected to the system.
- For Integrity NonStop NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series, the internal ServerNet fabric objects and a [VIO module](#) within each internal ServerNet fabric object.

G16SE Group

In AC-powered Integrity NonStop BladeSystems (except for NonStop BladeSystem NB50000c), Groups 110-115 can represent a 16-port Ethernet controller (G16SE), each of which contains two [VIO modules](#) (Modules 2 and 3).

Location in OSM Tree: System > Group 110-115 > VIO Module 2 and 3.

Attributes

Group

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Actions

Rediscover

Causes OSM to refresh and reanalyze the group and all subcomponents. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Hard Disk (CLIM)

A subcomponent of the [CLIM](#). For G2 and G5 CLIMs, there is only one hard disk object, located in Bay 1. For G6 and Gen8 CLIMs, there are two hard disks, located in Bay 1 and Bay 2.

Location in OSM Tree: System > CLIMs > CLIM > Hard Disk

Attributes

Hard Disk

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Firmware

Firmware Version	The version of the firmware running on the CLIM hard disk. Example: HPD5
------------------	---

Physical

Model	The model number of the CLIM hard disk that was assigned in manufacturing.
Serial Number	The serial number of the CLIM hard disk.

Logical

Device State	The state of the CLIM hard disk as known to the operating system on the server. Possible values include: OK, Warning, Fault, Off Duty, Not Installed.
--------------	---

Actions

Replace

Launches a guided procedure to make replacement of a CLIM hard disk drive more automated. If SNMP is not available and Hard Disk object is not displayed in the OSM Service Connection, the same guided procedure can be launched through the [Replace Hard Drive](#) on the [CLIM](#) object.

InfiniBand HCA Card (CLIM)

A subcomponent of the [CLIM](#) object for G6 CLIMs only.

Location in OSM Tree: System > CLIMs > CLIM > Infiniband HCA

Attributes

Infiniband HCA Card

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the InfiniBand HCA card as known to the operating system on the server. Possible values include: OK and Fault.
Node GUID	A text string displaying a globally unique identifier (GUID) for each InfiniBand HCA card, as assigned by the channel adapter vendor. It is obtained through an SNMP call. If the value is not available (for example, because the Maintenance Interface IP address is not available or the InfiniBand SNMP Agents are not functioning properly), it is displayed as "Not Available."
Number of Ports	The number of physical ports on the InfiniBand HCA card.
System Image GUID	A text string indicating the System Image GUID of the InfiniBand HCA. It is obtained through an SNMP call. If the value is not available (for example, because the Maintenance Interface IP address is not available or the InfiniBand SNMP Agents are not functioning properly), it is displayed as "Not Available."

Physical

Hardware Revision	A code that identifies the generation of the InfiniBand HCA Card. Hardware revision codes are used for tracking components.
Model	The model number of the InfiniBand HCA Card that was assigned in manufacturing.
Part Number	The part number of the InfiniBand HCA Card that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Serial Number	The serial number of the InfiniBand HCA Card.

Firmware

Compare State	Indication of the differences, if any, between the current and default InfiniBand HCA Card firmware versions. Values
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Version	The version of the InfiniBand HCA Card firmware running on the CLIM.

Actions

Firmware Update

Updates the firmware running on the InfiniBand HCA Card. Upon completion, OSM offers to reboot the CLIM, in order for the CLIM to start using the updated firmware.

Replace

Launches a service procedure that describes how to replace an InfiniBand HCA Card on a CLIM.

Internal ServerNet Fabric

The system has two internal ServerNet fabric objects, the Internal ServerNet X Fabric and the Internal ServerNet Y Fabric.

Each internal ServerNet fabric object can be expanded in the OSM tree pane to see the appropriate subcomponents (such as [processor switches](#) or [VIO modules](#)), depending on system type and configuration.

Location in OSM Tree: System > Fabric Group > Internal ServerNet Fabric

Example: Internal ServerNet Y Fabric

Attributes

None.

Actions

Group Connectivity ServerNet Path Test

You can perform this action on either the Internal ServerNet X Fabric or the Internal ServerNet Y Fabric. The action tests the links between SPs and ServerNet Switch Board maintenance entities (MEs) that provide ServerNet communication between groups on the system.

Processor-to-Processor Connectivity Test

Equivalent to the SCF STATUS SERVERNET command, this action tests the ServerNet connectivity between specified processor on this Internal Fabric. You can specify one or all processors. The action will report any ServerNet errors between the specified processor(s) and all other processors in the system.

Start ServerNet

Starts all ServerNet traffic through all or specified processors on the fabric.

Stop ServerNet

Stops all ServerNet traffic through all or specified processors on the fabric.

IO Module

A subcomponent of a [SAS Disk Enclosure](#).

Location in OSM Tree: System > SAS Disk Enclosures > SAS Disk Enclosure > IO Module

Attributes

None.

Actions

Replace

Launches a documented service procedure to replace an IO module in a SAS disk enclosure.

IOAM (I/O Adapter Module)

A modular I/O adapter module, compatible with both NonStop S-series and Integrity NonStop NS-series systems. There are two IOAMs in each [IOAM Enclosure](#).

Each IOAM contains:

- A [ServerNet Switch Board](#)
- Two [IOAM Power Supplies](#)
- Two [IOAM Fans](#)
- Up to five [FCSA](#) or [G4SAs](#)
- In an HP Integrity NonStop NS14000 or NS1000 system, slots 1 and sometimes 2 of each IOAM are occupied by a [4PSE](#) instead of an FCSA or G4SA.

NOTE: For an Integrity NonStop NS14000 or NS1000 system, an IOAM is displayed in the Multi-Resource Actions dialog box as an IO/Switch Module.

IOAMs are initially configured using the Configure Module action in the OSM Low-Level Link, as described in the *NonStop NS-Series Hardware Installation Manual* (available in the Hardware Service and Maintenance collection of NTL).

IOAM names in OSM include the group number and a module number of either 2 or 3. For example, IOAM 13.2 is located in group 13, module 2. The other IOAM in this IOAM group is IOAM 13.3.

NOTE: If for any reason a ServerNet switch board is not present in a module, the fans, power supplies, and adapters in that module will not appear in OSM.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM

Example: IOAM 13.2

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Actions

Read LCD

Displays all 16 lines of the IOAM's LCD text in the Action Detail dialog box.

Retrieve Network Connectivity Info

Displays remote IP addresses stored in the IPAUTH file of the processor switch.

Synchronize FIR Files to Other Switches

Synchronizes the FRU information record (FIR) files of the X and Y fabric processor switches.

Write LCD Line

Allows you to edit the text displayed by the IOAM's LCD. You can modify lines 9 through 15 with this action.

IOAM Enclosure

An enclosure that contains two [I/O Adapter Modules](#).

Location in OSM Tree: System > Group > IOAM Enclosure

Example: IOAM Enclosure 110

NOTE: For an Integrity NonStop NS14000 or NS1000 system, there is only one IOAM enclosure. In the OSM tree pane, it is located within the Fabric Group 100 object. In the Multi-Resource Actions dialog box, the IOAM enclosure is displayed as an IOAM/Switch Enclosure.

Attributes

IOAM Enclosure

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the IOAM enclosure is located. You can enter up to 15 alphanumeric characters.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the IOAM enclosure within the rack.
Locator	An optional text string assigned to further identify the physical location of the IOAM enclosure. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical Location action. This attribute is displayed only if a value is specified through the action.

Actions

Replace IOAM Enclosure or ServerNet Switch Board

Launches a guided procedure, which provides step-by-step instructions for replacing the entire IOAM enclosure or an individual ServerNet switch board within the enclosure.

NOTE: For an HP Integrity NonStop NS14000 or NS1000 system, there is only one IOAM enclosure, requiring an IOAM enclosure replacement to be done offline. Instead of a guided procedure, the replacement procedure for this type of system is documented in the Service Procedures section of the NTL Support and Service library, under NonStop NS-Series Hardware Servicing.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the IOAM enclosure:

- Rack Name is a user-defined name for the rack containing the IOAM enclosure. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the IOAM enclosure within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action will fail.
- Locator is an optional text string to help identify the physical location of the IOAM enclosure. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. An system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system while you create a physical view of your modular racks.

IOMF2 (I/O Multifunction 2)

Each I/O multifunction 2 (IOMF2) CRU in a NonStop server contains these components:

- A [service processor \(SP\)](#)
- Two internal [SCSI controllers](#)
- One external [SSAC](#)
- A ServerNet plug-in card ([PIC](#)), which provides connectivity to [internal ServerNet fabrics](#)

Location in OSM Tree: System > Group > Module > IOMF2

Slot Location: IOMF2 CRUs are located in slots 50 and 55 of Nonstop S-series I/O enclosures (service side).

Example: IOMF2 (1.1.55)

Attributes

IOMF2

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

DCC Voltage	The operational voltage of the IOMF2 CRU (specifically, the raw voltage supplied to the DC-to-DC converters).
Disabled ServerNet Ports	Which, if any, ServerNet router ports on this IOMF2 CRU are disabled. OSM actions to disable or enable a ServerNet port are performed as directed by OSM alarm repair actions.
Fan Voltage	The current voltage of the Fan CRU.
Main Rail Voltage	The voltage of the Main Rail, which supplies power to the IOMF2 CRU from its own power supply
Main Rail Voltage After Fuse	The current voltage on the Main Rail of the IOMF2 CRU, measured after the fuse.
MOSFET Voltage	The voltage measured between the MOSFET switch and the diode to the DCC. The MOSFET switch is located on the Other Rail between the alternate power supply and the DCC.

Other Rail Voltage	The voltage of the Other Rail, which connects the IOMF2 CRU to the other power supply in the enclosure (to provide power in the event of a problem with the Main Rail power supply).
Other Rail Voltage After Fuse	The current voltage on the Other Rail of the IOMF2 CRU, measured after the fuse.
Rail Maximum Voltage	The maximum voltage limit (60 volts) for the IOMF2 CRU.
Rail Minimum Voltage	The minimum voltage (39.6 volts) that must be available to power the IOMF2 CRU.
SCSI-X Voltage	The voltage of the SCSI-X path, the primary path used for disks on a system.
SCSI-Y Voltage	The voltage of the SCSI-Y path, the path configured for mirrored disks on a system.

Storage ASIC

Initialization State	The status of the storage ASIC in the CRU. Values: Initialized, Uninitialized, Unknown
----------------------	--

Actions

Disable ServerNet Port

Disables the specified ServerNet port on this CRU. Perform this action only as directed by OSM alarm repair actions.

Parameter: Port Number

Enable ServerNet Port

Enables the specified ServerNet port on this CRU. Perform this action only as directed by OSM alarm repair actions.

Parameter: Port Number

Force Power Off

This action is not supported for this CRU type. See the [Prepare to Power Off](#) action.

Power Off

This action is not supported for this CRU type. See the [Prepare to Power Off](#) action.

Prepare to Power Off

Performs precautionary check to make sure that you can safely remove the CRU.

The precautionary check makes sure that the other IOMF2 CRU in this enclosure exists and is powered on.

If the check confirms that you can safely power off the CRU, these preparatory steps are performed:

- If the SP on this IOMF2 is designated as Active (Primary), resets the SP so that the peer SP becomes primary
- Disables the battery

If the Prepare to Power Off action completes successfully, you can safely remove the CRU.

If the check fails, the Prepare to Power Off action fails, and you should perform the steps using other OSM actions before removing the CRU.

Replace

Launches the Replace IOMF guided procedure, which provides step-by-step instructions for replacing the IOMF2 CRU.

Storage ASIC Initialization Test

Prompts the storage subsystem manager process (\$ZZSTO) to initialize the storage ASIC in the CRU. If initialization fails, an alarm is generated.

This action is triggered automatically when a new CRU is inserted while OSM is running or when an (SCF) STATUS ADAPTER command is issued. If a CRU is inserted while OSM is not running, perform this action after logging on to the OSM Service Connection.

Test Verify

Performs basic tests on the CRU. You can perform this action when the CRU is online.

LIF

The logical interface, associated with a physical interface (PIF), used by an Ethernet controller port or a ServerNet adapter port.

Location in OSM Tree:

For a ServerNet adapter port LIF: System > Group > Module > adapter > SAC > PIF > LIF

Example: LIF \$ZZLAN.LAN01A

Attributes

LIF

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

LIF State	The state of the logical interface. Values: Started, Stopped, Unavailable
-----------	---

Actions

Abort

Terminates operation of the LIF. When the Abort action finishes, the LIF is in the Stopped state.

Delete

Deletes the LIF.

Start

Starts the LIF.

Stop

Rather than automatically stopping the LIF (as the Abort action does), this action first warns you if the LIF is currently in use (and stops it only after you confirm).

Logical Processor

The OSM Service Connection displays Logical Processor objects for both HP Integrity NonStop BladeSystems (J-series software) and Integrity NonStop NS-series servers (H-series software); what OSM displays depends on the type of system:

- For Integrity NonStop BladeSystems, OSM displays a Logical Processor object for each processor blade physically present in the [Enclosure](#).

Location in OSM Tree: System > Enclosure > Logical Processor

- For Integrity NonStop NS14000 series and NS16000 series servers, each [Blade Complex](#) consists of four Logical Processors (0, 1, 2, and 3). The Logical Processors are represented in each Blade Element by a Processor Element (PE) bearing the number of that particular Logical Processor. For example, PE 0 in Blade Element A represents Logical Processor 0 in that Blade Element. In OSM, PE attributes are displayed under the [Processor Components](#) object (located under Logical Processors) along with additional actions and attributes for the Logical Synchronization Unit (LSU).

Location in OSM Tree: System > Group > Logical Processor

- For Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC systems, each Blade Element contains only one Logical Processor. The Processor Components object displays processor attributes, but there are no PEs or LSUs.

Location in OSM Tree: System > Group > Logical Processor

Attributes

Logical Processor

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Halt Flag	Indicates whether a halt has occurred in this processor.
Halt Code	If a halt has occurred, this attribute displays the octal halt code associated with the halt flag. For more information on the halt code, see the <i>Processor Halt Codes Manual</i> .
Halt Subcode	If a halt has occurred, an octal value that represents the contents of a processor register known as the Lites Register.
Logical Processor State	The state of the logical processor, either Up or Down.
Number of Enabled Cores	Valid only for NonStop BladeSystem NB54000c and NB56000c, this attribute displays the number of licensed cores for this Logical Processor.
Number of IPUs	The number of IPUs (Instruction Processing Units) that make up this logical processor. This value is 2 if the processor is running as a 2-way SMP, 4 if the processor is running as a 4-way SMP, or 1 if the processor is not running SMP. NOTE: Displayed only for NonStop BladeSystem NB50000, NS2100, NS2200 series, NS2300, NS2400 series, and NS2000 series servers; not applicable for NonStop BladeSystem NB54000c and NB56000c or other NonStop NS-series servers.
Physical Cores	Valid only for NonStop BladeSystem NB54000c and NB56000c, this attribute displays the number of cores physically present for this Logical Processor.

Processor Blade	Valid only for NonStop BladeSystems, this attribute maps the Logical Processor to the Processor Blade it represents.
Processor Freeze State	Indicates whether the processor freeze state is enabled or disabled.
Processor State (from ME)	The state of the Logical Processor as seen by the Maintenance Entity (ME) of the associated ServerNet Switch Board. Values
Processor Type	The NonStop server type. Values Example: NSE-A
Redundancy State	Indicates whether the current processor configuration includes one (Simplex), two (Duplex), or three (Triplex) Blade Elements. NOTE: Valid for NS16000 series and NS14000 series servers only.
Total Memory Size	Total amount of memory on the processor. NOTE: Displayed only for (J-series) NonStop BladeSystems; not applicable for NonStop NS-series servers.
X Fabric ServerNet State	The state of the Internal ServerNet X Fabric. Values: Up, Disabled
Y Fabric ServerNet State	The state of the Internal ServerNet Y Fabric. Values: Up, Disabled

Physical

NOTE: Displayed only for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC servers.

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. NOTE: Not displayed for NS2100, NS2200 series, NS2300, or NS2400 series servers.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

X Fabric Connection

Port Name	The port on the Processor Switch to which the Logical Processor is connected on the X Fabric.
-----------	---

Y Fabric Connection

Port Name	The port on the Processor Switch to which the Logical Processor is connected on the Y Fabric.
-----------	---

Actions

Disable Processor Freeze

Turns the Freeze Enable flag on this processor off. A freeze-disabled processor is unaffected when any other processor halts or the (Low-Level Link) system-level **Freeze** action is performed.

Enable Processor Freeze

Turns the Freeze Enable flag on this processor on. If the OSM Low-Level Link **System Freeze** attribute is set to Enabled, a freeze-enabled processor might freeze if either another freeze-enabled processor halts, or the (Low-Level Link) system-level **Freeze** action is performed.

Halt

Terminates all processes running on this processor. Halting a processor does not affect any other processors in the system.

⚠ CAUTION: Halting a processor might result in unrecoverable loss of data. Use the Halt action only to prepare for reloading the processor or for performing a memory dump.

Power Cycle LSU

Performs a hard down action on all connected ports (X and Y), waits briefly, and then reenables the connected ports.

NOTE: This action is available for Integrity NonStop NS16000 and NS14000 series servers only.

Reclaim Memory Pages

Use as directed, by the repair actions for the “Too Many Corrected Memory Errors” alarm, to avoid a processor outage for a processor reload that would otherwise be necessary to reclaim the removed pages.

NOTE: This action is valid for Integrity NonStop NS16000 and NS14000 series servers only; it will fail for all other server types.

Reload

Based on selected parameters, loads the processor.

A dialog box prompts you to specify:

- Prime: Whether or not to prime for reload. Do not select PRIME if that operation has already been performed on the processor.
- Switch: Whether or not to allow automatic switching of disk paths (for load balancing).
- Exclude PE from Load: Whether or not to exclude the processor element (PE) for a specified Blade Element from the reload, for the purpose of dumping that PE before reintegrating it. The options include PE A, PE B, PE C, or Any PE. If the Any PE option is selected, OSM automatically chooses a PE to exclude from the reload operation.

NOTE: The Exclude PE from Load option is valid for NS16000 series and NS14000 series servers only.

- Fabric (X, Y, or default).
- Optional alternate OS file set volume or file.

For more information on dumping and reloading processors, see the *NonStop NS-Series Operations Guide*.

Responsive Test

Verifies that the processor is connected and responding.

Soft Reset

Used following a firmware update action on the millicode for the changes to take effect.

Maintenance PIC

Located in slot 1 of a processor switch in NonStop NS-series servers that contain processor switches.

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether or not the power supply's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Model	Identifies the plug-in card type as being a Maintenance PIC.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indicates whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Actions

Replace

Invokes a guided procedure that helps to replace the switch PIC.

Set LED State

Turns on or off the amber LED located on the PIC. The current state is indicated by the [LED State](#) attribute.

Maintenance Switch

An Ethernet switch that allows the OSM console to communicate with the Maintenance Entity (ME) in the [ServerNet switch board](#).

Location in OSM Tree: System > Monitored Service LAN Devices > Maintenance Switch

Example: Maintenance Switch SRSLAN

Attributes

Maintenance Switch

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Configured System Name	A configurable name assigned through the switch's web interface, launched by the Link to Web Interface action.
Contact	Configurable contact name set in the web interface (launched by the Link to Web Interface action) by selecting Configuration tab > System Info > System Contact.
Device Status	Indicates whether the switch is up or down.

Firmware Revision	The version of the firmware running on the switch.
IPv4 Address	The IPv4 address of the switch.
Lines Connected	Lists the port numbers of ports on the switch that have lines connected.
Lines Disconnected	Lists the port numbers of ports on the switch that have been disconnected (since the OSM server has been running).
Location	Configurable location identifier set in the web interface (launched by the Link to Web Interface action) by selecting Configuration tab > System Info > System Location.
MAC Address	The media access control (MAC) address of the switch.
Model	Hardware model information for the ProCurve switch.
Part Number	The part number of the component that was assigned in manufacturing. Not displayed for ProCurve 2510 switches; see Model attribute for switch model details.
ROM Version	The version of the startup bootcode for the switch.
Serial Number	A unique identification number assigned to each switch in manufacturing.

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the maintenance switch is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the maintenance switch within the rack.

Actions

Link to Web Interface

Opens a Web interface that provides detailed device configuration and information for the maintenance switch.

Rediscover

Causes OSM to refresh and reanalyze the object. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Stop Monitoring

Stops OSM from monitoring the maintenance switch.

Memory Card (Blade Element)

In the OSM Service Connection, Memory Card objects are displayed as subcomponents under the:

- [Blade Element](#) object for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC servers.

Location in OSM Tree: System > Blade Complex > Blade Element > Memory Card

- [Processor Blade](#) object for Integrity NonStop BladeSystems.

Location in OSM Tree: System > Enclosure > Processor Blade > Memory Card

Attributes

Memory Card

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Actions

Replace

Launches a documented service procedure to replace the memory card in the processor blade.

NOTE: Displayed only for (J-series) NonStop BladeSystems; not applicable for NonStop NS-series servers.

Module

A set of components that share a common hardware interconnection, such as a backplane. This object applies only to Nonstop S-series processor and I/O enclosures, in which each enclosure contains one [group](#), and a group contains only one module. The module is considered a subcomponent of the group. IOAM enclosures contain two [I/O adapter modules](#).

Example: Module 2.1

Attributes

Module

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the module is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the module within the rack.
Locator	An optional text string assigned to further identify the physical location of the module. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical

	Location action. This attribute is displayed only if a value is specified through the action.
--	---

Temperature Sensor

Current Value	The current temperature, in degrees Celsius (°C), inside the enclosure of the module.
---------------	---

Actions

Rediscover

Causes OSM to refresh and reanalyze all components within the module. Use this action in situations such as:

- OSM does not recognize a new CRU following a CRU replacement.
- An alarm remains after the alarm condition has been fixed.

Redundant Power Scrub

Tests fault tolerance of the power environment within the module. If the results of the action indicate a problem, check the Power State attribute of the individual CRUs to determine where the problem lies.

This action is run automatically at 2:00 a.m. daily. It can also be performed manually at any time. See note below for default value of the new Redundant Power Scrub test.

On T0682AAC and later, this OSM action is also supported on Telco systems.

NOTE: A new version of Redundant Power Scrub is available in T0682 ABE and later. It provides independent battery testing and an extended load test for the bulk power supplies. With this new version, the action can take up to 25 minutes to complete. The new battery scrub is significantly enhanced in its ability to detect weak or failed batteries. For systems with many old batteries (over 5 years old), the battery scrub might call out multiple batteries for replacement.

To use this new functionality, in addition to installing OSM T0682 ABE or later, you must:

- Update all enclosures with a new PIB-to-PIB crossover cable (see FCO 44440).
- Add "PowerScrubVersion = 3" parameter to your OSMCONF file.

The default test interval for this new version is 7 days instead of 24 hours.

For information on creating and using an OSMCONF file or changing default values for this or other parameters, see the *OSM Configuration Guide*.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the module:

- Rack Name is a user-defined name for the rack containing the module. You can enter up to 15 alphanumeric characters.
- Rack Offset allows you to display a numerical value representing the location of the module within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action will fail.
- Locator is an optional text string to help identify the physical location of the module. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. A system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware

error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

Monitored Service LAN Devices

Contains [Maintenance Switch](#), [Fibre Channel Router](#), [UPS](#), and (Telco) [Alarm Panel](#) objects that you have configured OSM to monitor through the actions on this object.

Location in OSM Tree: System > Monitored Service LAN Devices

Attributes

None.

Actions

Start Monitoring Alarm Panel

Valid for Telco systems only – Causes the OSM Service Connection to display and start monitoring the [Alarm Panel](#). You are prompted to enter the IPv4 address of the alarm panel, a name (between 1 and 60 characters, to be displayed by OSM as part of the maintenance switch object name), and appropriate group name for SNMP Read Access Community.*

Start Monitoring Fibre Channel Router

Causes the OSM Service Connection to display and start monitoring the fibre channel router. You are prompted to enter a User ID and Password (which are established by the administrator during initial configuration of the fibre channel router), the IPv4 address of the fibre channel router, and a name (between 1 and 60 characters, to be displayed by OSM as part of the fibre channel router object name).

Start Monitoring Maintenance Switch

Causes the OSM Service Connection to display and start monitoring the maintenance switch. You are prompted to enter the IPv4 address of the maintenance switch, a name (between 1 and 60 characters, to be displayed by OSM as part of the maintenance switch object name), and appropriate group name for SNMP Read Access Community.*

NOTE: * SNMP Read Access Community user groups and access privileges are established by the administrator for the maintenance switch. For information on how an administrator configures user groups, see the *OSM Configuration Guide*.

Start Monitoring UPS

Causes the OSM Service Connection to display and start monitoring the UPS. You are prompted to enter the IP address of the UPS, a name (between 1 and 60 characters, to be displayed by OSM as part of the UPS object name), and appropriate group names for SNMP Read Access Community and SNMP Write Access Community.*

NOTE: * SNMP Read Access Community and SNMP Write Access Community user groups and access privileges are established by the administrator for the UPS. For information on how an administrator configures these user groups, see the *OSM Configuration Guide*.

Motherboard (CLIM)

A subcomponent of G6 and Gen8 [CLIMs](#).

Location in OSM Tree: System > CLIMs > CLIM > Motherboard

Attributes

None.

Actions

Replace

Launches a documented service procedure to replace a CLIM motherboard.

NIC (CLIM)

A subcomponent of the [CLIM](#).

For Gen8 CLIMs, there are three types of NIC cards, as identified by the Model and Part Number attributes. The Models are:

- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP NC560SFP+ 1GbE NIC
- HP Ethernet 1Gb 2-port 332T Adapter (HP NC332T NIC)

Location in OSM Tree: System > CLIMs > CLIM > NIC

Attributes

NIC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the NIC as known to the operating system on the server. Possible values include: OK and Fault.
--------------	---

Physical

Model	The model number of the CLIM NIC that was assigned in manufacturing.
Part Number	Displayed only for NICs on a Gen8 CLIM, this represents the part number of the NIC assigned in manufacturing, and used for identifying and ordering a replacement.

Firmware

Compare State	Indication of the differences, if any, between the current and default NIC firmware versions. Values
Default File Name	The name of the file to be used for an NIC firmware update.
Default File Version	The version of the firmware to be used for an NIC firmware update.
Version	The version of the NIC firmware running on the CLIM.

Actions

Firmware Update

Updates the firmware running on the NIC. Upon completion, OSM offers to reboot the CLIM, in order for the CLIM to start using the updated firmware.

Replace

Launches a documented service procedure to replace a NIC in a CLIM.

Optical Extender PIC

These (optional) Optical Extender PICs are used only in HP Integrity NonStop systems that include VIO enclosures (represented in the OSM Service Connection as [VIO modules](#)). Optical Extender PICs can be used as follows:

- Slot 2 – for additional processor connectivity (processors 4 through 7) on NS14000 series, NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series servers.
- Slot 3 – for NonStop S-series connectivity on NS3000AC, or for CLIM connectivity on NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series servers.
- Slot 4 – for CLIM connectivity on NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series servers.
- Slot 5 – for ServerNet cluster connectivity on NonStop NS14000 series servers.

Each Optical Extender PIC contains four [ports](#).

NOTE: Optical Extender PICs are not a subcomponent of VIO modules in S-series servers.

For more information on ServerNet cluster connectivity for VIO enclosures, see the *ServerNet Cluster Supplement for NS-Series*.

Location in OSM Tree: System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > Optical Extender PIC

Example: Optical Extender PIC (100.2.2)

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether or not the Optical Extender PIC's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indicates whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Type	Identifies the type of ServerNet PIC. Value: Optical Extender PIC

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Power Off

Shuts off power to the Optical Extender PIC.

Power On

Restores power to the Optical Extender PIC.

Replace

Launches a service procedure describing how to replace an Optical Extender PIC.

Set LED State

Turns on or off the amber LED located on the Optical Extender PIC. The current state is indicated by the [LED State](#) attribute.

PCI Riser

A subcomponent of the [CLIM](#). Only one PCI Riser can be installed in G2, G5, and Gen8 CLIMs; up to two PCI Risers can be installed in G6 CLIMs.

Location in OSM Tree: System > CLIMs > CLIM > PCI Riser

Attributes

PCI Riser

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Actions

Replace

Launches a documented service procedure to replace a PCI Riser in a CLIM.

PIC

A replaceable component of an [IOMF2](#) CRU that provides connectivity to internal ServerNet fabrics.

Location in OSM Tree: System > Group > Module > IOMF2 > PIC

Example: PIC (1.1.52.1)

Attributes

PIC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Type	Indication of the type of plug-in card. Values: NNA, Serial Copper, ECL, Long-Haul Fiber, Short-Haul Fiber
------	--

Logical

Connector Number	A unique number used to distinguish between plug-in cards on an MSEB CRU.
------------------	---

Actions

Clear Loopback Test

Clears the loopback test on a plug-in card (PIC). This action clears both the internal loopback test initiated by the Internal Loopback Test action and the external loopback initiated by the guided procedure for troubleshooting a ServerNet fabric. The action enables ServerNet ports so that packets can be routed to the PIC from adjacent ports on the MSEB or IOMF2 and from the PIC in another enclosure connected by the ServerNet cable to the PIC being tested. Use this action if the \$ZCMOM process terminates while a loopback test is being performed. This action is safe to use on any PIC even if you are not sure a loopback test needs to be cleared on the PIC.

Enable/Disable Port

Enables or disables the port for this CRU.

Parameter: Enabled (true = enabled, false = disabled)

NOTE: If the port being enabled or disabled is on an NNA-type (MSEB) PIC connected to an External Servernet Switch, you must issue a Reset on the Primary SP in Group 1.

External Loopback Test

The external loopback test checks the circuitry of a plug-in card (PIC) to determine if ServerNet traffic can pass through the PIC. You can use this test on a PIC installed in any port of an MSEB or IOMF2 CRU. This test requires you to remove the ServerNet cable attached to the PIC and install a loopback plug.

The external loopback test indicates whether or not the PIC circuitry is operational or faulty. Unlike the internal loopback test, the external loopback test also checks the connector on the PIC.

⚠ CAUTION: Do not use the external loopback test on a PIC that you believe is operating normally. Doing so shuts down ServerNet traffic through the PIC for the duration of the test (several minutes). The action isolates the MSEB port occupied by the PIC, preventing the port from sending or receiving ServerNet traffic. ServerNet traffic resumes when the test is finished.

Do not use the external loopback test if alarms are present on the peer fabric (the fabric opposite the PIC you intend to test). If you do so, you might lose access to both fabrics, thereby isolating the enclosure from the rest of the system. Multiple enclosures can be lost in this manner.

When to Use the External Loopback Test

Typically, you use the external loopback test to isolate the cause of a malfunctioning ServerNet link where a PIC is part of that path. Use this test if you have run the internal loopback test on a PIC, and the test passed, but you believe the PIC might still be bad. If both PICs of a ServerNet link pass the external test, but the link is not usable, probably the ServerNet cable is faulty.

Internal Loopback Test

Tests the circuitry of a plug-in card (PIC) installed in an MSEB to determine if ServerNet traffic can pass through the PIC.

⚠ CAUTION: Do not perform this test on a PIC that is operating normally because it will shut down ServerNet traffic through the PIC. Also, do not perform this test on an NNA-type ServerNet PIC because the test will fail even if nothing is wrong with the NNA PIC.

NOTE: This test fails if no device is attached to the PIC even if nothing is wrong with the PIC itself.

PIF

Physical interface (PIF) objects are the ports on these resources through which LAN connections are made:

- Ethernet ServerNet addressable controllers (E4SA SACs)
- Fast Ethernet ServerNet addressable controller (FESA SACs)
- Gigabit Ethernet ServerNet addressable controllers (GESA SACs)
- Common Controller ServerNet addressable controllers (CCSA SACs)
- Token Ring ServerNet addressable controllers (TRSA SACs)

Location in OSM Tree: System > Group > Module > CRU > SAC > PIF

Example: TRSA PIF \$ZZLAN.TRSA0.0.B

Attributes

PIF

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Current Configured Speed	Valid only for FESA and GESA PIFs. The transmission rate for the ServerNet addressable controller.
Device State	The state of the component as known to the operating system on the server. Values
Duplex Mode	The transmission mode for the ServerNet addressable controller. Values: Half Duplex, Full Duplex, Unknown
Hardware MAC Address	The media access control (MAC) address of the PIF hardware.
Interface Type	Displayed for CCSA PIFs only.
Maximum Speed	The maximum transmission rate for the ServerNet addressable controller. Values: 10 megabits per second, 100 megabits per second, Unknown
Network MAC Address	The media access control (MAC) address of the PIF network.
Processors with Data Path	The processor numbers for processors that have a successful data path to the PIF. If no processor has a path, "None" is shown. Example: (0,1)
Ring State	Valid only for the TRSA CRU. The current state of the Token Ring. Values: Opened, Opening, Open Failure, Closed, Closing, Ring Failure
Ring Open Status	Valid only for the TRSA CRU. Status (success or reason for failure) of the most recent attempt to enter the Token Ring.

	Values: Last Open Successful, No Open Attempted, Bad Parameter, Lobe Failed, Signal Loss, Insertion Timeout, Ring Failure, Beaconsing, Duplicate MAC, Request Failed, Remove Received
Link Pulse State	Valid only for E4SA PIFs. A value of Up confirms that the cable from the PIF to the LAN is connected and operational. A value of Down indicates a problem with LAN connectivity.

Actions

Abort

Terminates operation of the PIF. When the Abort action finishes, the PIF is in the Stopped state.

Configure LIF

Configures the associated [LIF](#).

Start

Starts the CRU's PIF. The PIF must be in the Stopped state before you perform this action. When the Start action completes, the PIF is in the Started state.

Stop

Rather than automatically stopping the PIF (as the Abort action does), this action first warns you if the PIF is currently in use (and stops it only after you confirm).

PMCU

The power monitor and control unit (PMCU) controls and monitors the battery connection to the DC power distribution buses. Along with the service processor, the PMCU diagnoses the condition of the batteries, fans, and power supplies and regulates the voltage supplied to the fans.

Location in OSM Tree: System > Group > Module > PMCU

Slot Location: PMCUs are located in slots 21 and 22 of Nonstop S-series I/O enclosures (appearance side).

Example: PMCU (1.1.21)

Attributes

PMCU

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Temperature Sensor

Normal Minimum Value	The minimum acceptable air intake temperature is 5 degrees Celsius. If the temperature falls below 5 degrees, an alarm is generated.
Current Value	The current temperature, in degrees Celsius (°C), inside the enclosure of the module.
Normal Maximum Value	The maximum acceptable air intake temperature is 50 degrees Celsius. If the temperature rises above 50 degrees, an alarm is generated.

Actions

None.

Power Supply

The power supply converts standard AC line voltage and distributes DC power to all components in its power domain. The power supply is a separate CRU for enclosures containing IOMF2 CRUs. In DC-powered Telco systems, the power supply units displayed in slots 31 and 32 of the OSM GUI represent up to 4 Telco Isolating Converters (TICs) in positions A1, A2, B1, and B2. For information on installing or replacing power components in a Telco system, see the *NonStop S-Series Central Office Server Installation and Service Guide*.

Location in OSM Tree:

CRU: System > Group > Module > Power Supply

Slot Location:

CRU: Power supply CRUs are located in slots 31 and 32 of enclosures containing IOMF2 CRUs.

Example: Power Supply (1.1.31)

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Power State	The state of the power supply CRU as known to the operating system on the server. Values NOTE: Not displayed for an IOMF or NonStop S7000 PMF CRU.

Logical

Enabled State	The initial state of the power supply component at the time of discovery. Values
Device State	The state of the component as known to the operating system on the server. Values

Actions

Replace

Launches an interactive action to guide you through replacement of a power supply CRU. This action is applicable for IOMF2 and most PMF enclosures. It is not applicable for S7000 PMF or IOMF CRUs (in which the power supply is not a customer-replaceable unit). The steps include:

NOTE: In DC-powered Telco systems, instead of having power supply units in slots 31 and 32, there are actually 4 TICs (in positions A1, A2, B1, and B2). If the system is not wired as documented in the *NonStop S-Series Central Office Server Installation and Service Guide*, OSM cannot properly identify the TIC that needs to be replaced. If an OSM alarm appears on a power supply in either slot 31 or 32, consult your wiring diagram and the *NonStop S-Series Central Office Server Installation and Service Guide* before replacing a power supply component.

1. Preparing to replace the power supply CRU – The action directs you to the [Replacement Guidelines and Precautions](#) help topic for guidelines and precautionary steps to observe before and during the CRU replacement.
2. After clicking **Yes** to confirm that you are ready to proceed with the replacement action:
 - OSM checks the peer power supply to verify that it is functional and can take over during the replacement.
 - If the peer power supply is functional, OSM disables the battery associated with the power supply CRU to be replaced.
 - If these tasks complete successfully, a dialog box informs you that the power supply is ready to be replaced.
3. After replacing the power supply CRU, click **Continue** to complete the action. OSM verifies the status of the new power supply. If it is functional, OSM enables the battery that was disabled earlier in the procedure.

If at any point during the procedure OSM finds problems that prevent the action from completing (or make continuing inadvisable), a dialog box reports the problems that must be addressed before the CRU replacement can be safely completed.

Replacement Guidelines and Precautions

Preparing to Replace the Power Supply

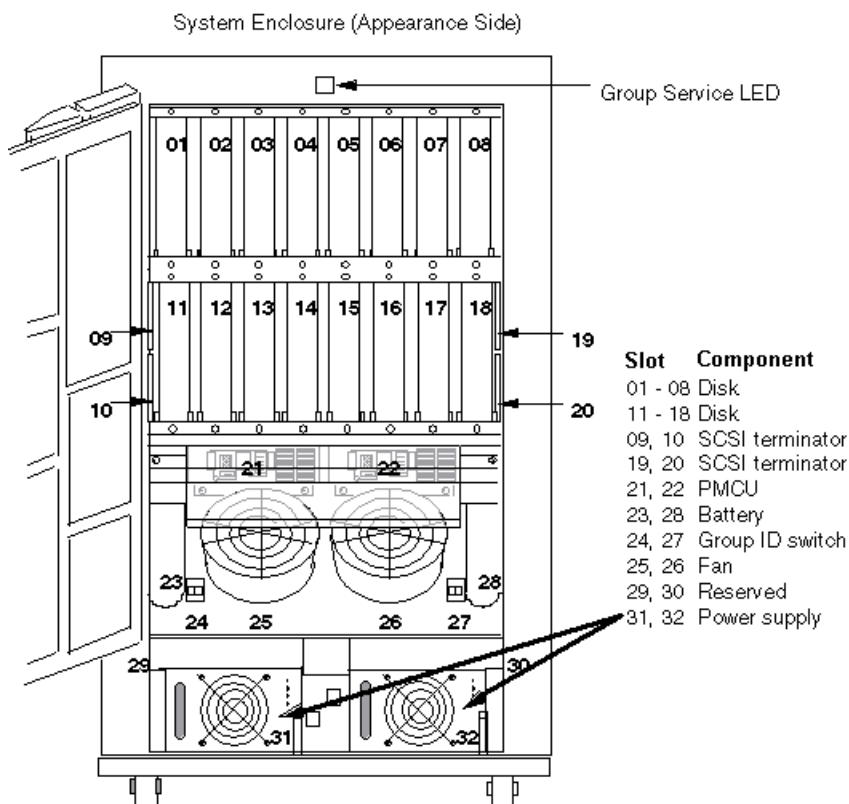
Perform these preparatory steps before you attempt to replace a power supply:

1. Review these important notes and cautions:
 - Before handling any CRU, obtain an electrostatic discharge (ESD) protection kit. Follow the directions on the kit for replacing a CRU to prevent damage to system components.
 - Power cords might contain faulty connectors that, when touched, vibrated, or flexed, can cause intermittent power or the loss of a processor.
 - Before replacing a power supply, visually check the power cord without touching the power cord. If the power cord molding is elliptical rather than square, or if the power cord part number is TPN 064583, you must replace the power cord offline with power cord TPN 421575 before you can replace the power supply. For power cord replacement instructions, refer to the Support and Service > Service Procedures collection of NTL. If you are replacing both the power cord and the power supply, install the replacement power cord before installing the replacement power supply.

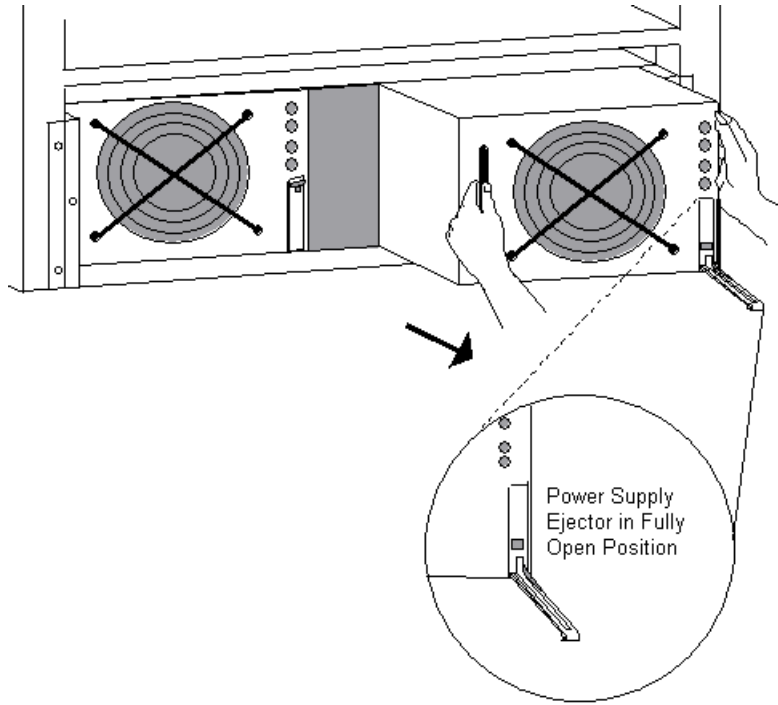
- Handle with care – the power supply weighs approximately 5.6 kilograms (14 pounds).
- Follow these standard operating practices when replacing CRUs:
 - Replace only one CRU at a time. Attempting to replace more than one hardware component at a time might cause serious system outages, processor halts, and connectivity problems.
 - Remove all jewelry and metal accessories, such as rings, watches, and necklaces, before working with the equipment. These items can damage electrical equipment or result in personal injury.
 - Restrain any dangling items that can get caught in electromechanical equipment, such as long hair and sleeves, before working with the equipment.
- 2. Unpack and inspect the replacement power supply. Use a flashlight to examine the pins on the power supply's backplane connector for any damage. If any pins are bent or broken, you must order another power supply (or have the backplane connector repaired or replaced) before continuing with this procedure. Refer to *Avoiding Connector and Backplane Damage During CRU/FRU Replacement* in the Support and Service > Service Procedures collection of NTL.

Removing the Power Supply

1. Remove the front panel from the power shelf.
2. Locate the power supply you are removing (power supplies are in slots 31 and 32). At this point, the LED above the power supply you are removing might or might not be lit. This illustration shows an S7x000 processor enclosure. For an illustration of an IOMF2 CRU, see the *NonStop S-Series Hardware Installation and FastPath Guide*.



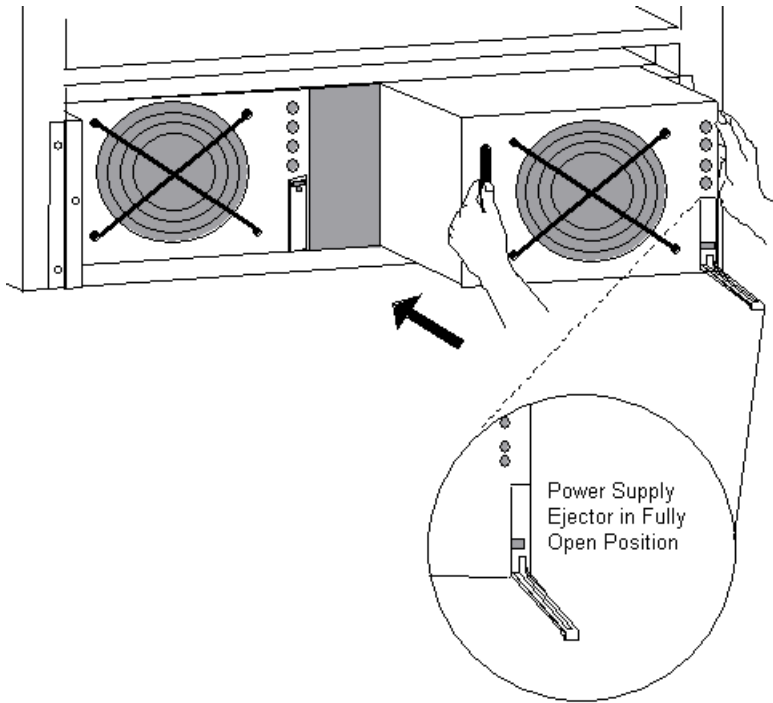
3. Lower the ejector on the power supply to its fully open position. This action disconnects the power supply from the power interface board (PIB) and the AC power cord directly behind it.



4. With one hand, grasp the handle of the power supply and slide the power supply partway out of the slot.
5. Using your other hand to support the weight of the power supply, slide the power supply all the way out of the slot.

Installing the Replacement Power Supply

1. Lower the ejector on the replacement power supply to its fully open position.



2. With one hand, grasp the handle of the power supply. Use your other hand to support the weight of the power supply. Then slowly push the power supply all the way into the empty slot.
3. Raise the ejector on the replacement power supply to its fully closed position. This action connects the power supply to the power interface board (PIB) and the AC power cord directly behind it.

The green power-on LED above the replacement power supply should now be lit. If the LED is not lit, either reseal the power supply or install a different power supply.

4. Replace the front panel on the power shelf.
5. Return to the OSM Service Connection Actions dialog box and click **Continue** to indicate that you have completed the physical CRU replacement. OSM then verifies the status of the new power supply. If it is found to be functional, OSM enables the associated battery that was disabled earlier in the procedure.

Power Supply (Blade Element)

Subcomponent of a [NonStop Blade Element](#). There are two power supplies in each enclosure.

Location in OSM Tree: System > Group > Blade Complex > Blade Element > Blade Element Power Supply

Example: Blade Element Power Supply (400.1.3)

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Device State	The state of the Blade Element Power Supply, as known to the operating system on the server. Possible values include OK, Fault, Power Loss, and Power Supply Fan Fault.
Manufacturer	Identifies the manufacturer of the component. Displayed for NonStop NS14000 series and NS16000 series servers only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. NOTE: Not displayed for NS2100, NS2200 series, NS2300, or NS2400 series servers.
Serial Number	The serial number of the component assigned to it by the supplier of the component. Displayed for NonStop NS14000 series and NS16000 series servers only.

Actions

Replace

Displays a procedure for replacing the Blade Element power supply.

Power Supply (CLIM)

A subcomponent of the [CLIM](#).

Location in OSM Tree: System > CLIMs > CLIM > Power Supply

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the component as known to the operating system on the server. Possible values include: OK, Degraded, Fault, Not Installed.
--------------	---

Actions

Replace

Launches a documented service procedure to replace a power supply unit in a CLIM.

Power Supply (FCDM)

Subcomponent of a [FCDM](#). There are two power supplies in each FCDM.

Location in OSM Tree: System > Group > FCDM Collection > FCDM > Power Supply

Example: Power Supply (111.211.1.95)

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

LED State	Indicates whether or not the power supply's (amber) fault LED is blinking. Value: Blinking or Off
Type	The vendor hardware type.

Logical

AC Power State	Whether the power source is On or Off.
Device State	The state of the component as known to the operating system on the server. Values
Vendor Hardware Revision	A code that identifies the generation of the component provided by its supplier.

Actions

Blink LED Off

Turns off the blinking of the power supply's (amber) fault LED.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED OFF

Blink LED On

Causes the power supply's (amber) fault LED to start blinking.

SCF Equivalent: SCF Control SAC \$ZZSTO.#sac-name, deviceid(shelf,bay), LED ON

Replace

Displays the procedure for replacing the power supply.

Power Supply (IOAM)

Supplies power to the [IOAM](#). There are two IOAM power supply units in each IOAM.

For information on how to replace an individual Power Supply, see the Support and Service > Service Procedures collection in NTL.

NOTE: If a ServerNet switch board is not present, the IOAM power supplies will not appear in OSM.

Location in OSM Tree: System > Group > IOAM Enclosure > IOAM > Power Supply

Example: Power Supply (13.2.15)

Attributes

IOAM Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Serial Number	The serial number of the component assigned to it by the supplier of the component.
Type	The vendor hardware type.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Configuration

These attributes are applicable only for an IOAM enclosure in an HP Integrity NonStop NS14000 or NS1000 system:

Power Source	Indicates the state of this power supply unit's backup power configuration as known to OSM. Values: Not Configured, AC, UPS, Unknown You must use the Configure Power Source as UPS action to set this value to UPS in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS.
UPS IPv4 Address	The IPv4 address of the UPS configured to provide backup power in the event of a power failure, if specified through the Configure Power Source as UPS action.

Actions

None for HP Integrity NonStop NS5000 or NS16000 series servers.

For an IOAM enclosure in an HP Integrity NonStop NS14000 or NS1000 system only, these actions are available:

Configure Power Source as AC

Sets the Configuration > Power Supply attribute value for this power supply unit to AC. You must be logged on as super.super to perform this action.

Configure Power Source as UPS

Sets the Power Source attribute value for this power supply unit to UPS. You must be logged on as super.super to perform this action. Upon initiating the action, you are prompted to enter the IPv4 address of the UPS.

For an Integrity NonStop NS14000 or NS1000 system, you must use this action to configure at least one of your IOAM power supplies (to specify UPS as the backup power source) in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your UPS. For more information on preparing for AC power-fail scenarios, see the *NonStop NS14000 or NS1000 Planning Guide*. For more information on using the POWERFAIL_DELAY_TIME command to specify the Power-Failure-to-Shutdown time interval, see the *SCF Reference Manual for the Kernel Subsystem*.

Delete the Power Source Configuration

Sets the Configuration > Power Supply attribute value to Not Configured. You must be logged on as super.super to perform this action.

Power Supply (Processor Switch)

One of two FRUs that supply power for the components in a processor switch.

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether or not the power supply's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Configuration

Power Source	Indicates the state of this power supply unit's backup power configuration as known to OSM. Values: Not Configured, AC, UPS, Unknown You must use the Configure Power Source as UPS action to set this value to UPS in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS.
UPS IPv4 Address	The IPv4 address of the UPS configured to provide backup power in the event of a power failure, if specified through the Configure Power Source as UPS action.

Actions

Configure Power Source as AC

Sets the Configuration > Power Supply attribute value to AC. You must be logged on as super.super to perform this action.

Configure Power Source as UPS

Sets the Power Source attribute value for this power supply unit to UPS. You must be logged on as super.super to perform this action. Upon initiating the action, you are prompted to enter the IPv4 address of the UPS.

For Integrity NonStop NS16000 series servers, you must use this action to configure at least one of your processor switch power supplies (to specify UPS as the backup power source) in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the

powerfail-delay time interval specified for your UPS. For more information on preparing for AC power-fail scenarios, see the *NonStop NS 16000 Series Planning Guide*. For more information on using the POWERFAIL_DELAY_TIME command to specify the Power-Failure-to-Shutdown time interval, see the *SCF Reference Manual for the Kernel Subsystem*.

Delete the Power Source Configuration

Sets the Configuration > Power Supply attribute value to Not Configured. You must be logged on as super.super to perform this action.

Replace

Launches the guided procedure to replace a processor switch power supply.

Set LED State

Turns on or off the amber LED located on the PIC port. The current state is indicated by the [LED State](#) attribute.

Power Supply (SAS Disk Enclosure)

A subcomponent of a [SAS Disk Enclosure](#).

System > SAS Disk Enclosures > SAS Disk Enclosure > Power Supply

Attributes

None.

Actions

Replace

Launches a documented service procedure to replace a power supply in a SAS disk enclosure.

Power Supply and Fan (Telco SAS Disk Enclosure)

In the OSM Service Connection, a subcomponent displayed for a Telco [SAS Disk Enclosure](#) only. In commercial SAS Disk Enclosures, [SAS Power Supplies](#) and [SAS Fans](#) are represented by separate objects in OSM.

System > SAS Disk Enclosures > SAS Disk Enclosure > Power Supply and Fan

Attributes

None.

Actions

Replace

Launches a documented service procedure to replace a power supply or fan in a Telco SAS disk enclosure.

Power Supply (VIO)

Provides power to the VIO enclosure (represented in the OSM Service Connection as a [VIO module](#)). There are two VIO power supplies in each VIO enclosure.

Attributes

VIO Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component. Displayed for VIO power supplies in S-series VIO modules only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Configuration

NOTE: These attributes are not displayed for a power supply unit in an S-series VIO Module.

Power Source	Indicates the state of this power supply's backup power configuration as known to OSM. Values: Not Configured, AC, UPS, Unknown You must use the Configure Power Source as UPS action to set this value to UPS in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your rack-integrated UPS.
UPS IPv4 Address	The IPv4 address of the UPS configured to provide backup power in the event of a power failure, if specified through the Configure Power Source as UPS action.

Actions

Configure Power Source as AC

Sets the Configuration > Power Supply attribute value for this power supply to AC. You must be logged on as super.super to perform this action.

NOTE: This action is not valid for a power supply unit in an S-series VIO Module.

Configure Power Source as UPS

Sets the Power Source attribute value for this power supply to UPS. You must be logged on as super.super to perform this action. Upon initiating the action, you are prompted to enter the IPv4 address of the UPS.

You must use this action to configure at least one of your VIO power supplies (to specify UPS as the backup power source) in order for OSM to provide an orderly system shutdown in the event that a power failure exceeds the powerfail-delay time interval specified for your UPS. For more information on preparing for AC power-fail scenarios, see the Planning Guide for your NonStop system. For more information on using the POWERFAIL_DELAY_TIME command to specify the Power-Failure-to-Shutdown time interval, see the *SCF Reference Manual for the Kernel Subsystem*.

NOTE: This action is not valid for a power supply unit in an S-series VIO Module.

Delete the Power Source Configuration

Sets the Configuration > Power Supply attribute value to Not Configured. You must be logged on as super.super to perform this action.

NOTE: This action is not valid for a power supply unit in an S-series VIO Module.

Replace

Displays a service procedure describing how to replace a power supply in a VIO enclosure.

Processor (CLIM)

A subcomponent of the [CLIM](#).

Location in OSM Tree: System > CLIMs > CLIM > Processor

Attributes

Processor

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Model	The model number of the CLIM processor that was assigned in manufacturing.

Logical

Current Speed	The processor speed.
Device State	The state of the CLIM processor as known to the operating system on the server. Possible values include: OK, Degraded, Fault, Off Duty.

Actions

Replace

Launches a documented service procedure to replace a processor in a CLIM.

Processor Blade

This object represents one of the eight processor blades in an Integrity NonStop blade server. There can be one or two Integrity NonStop blade servers in an Integrity NonStop BladeSystem. In the OSM Service Connection, the Processor Blade objects are found within the [Enclosure](#) object, which represents each blade server.

Within each Processor Blade object, OSM displays eight [Memory Cards](#) and a [ServerNet Interface Card](#).

Location in OSM Tree: System > Enclosure > Processor Blade

Attributes

Processor Blade

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Product Name	The product name of the component as assigned by the manufacturer.
Replacement Part Number	The replacement part number of the component.
Serial Number	The serial number of the component assigned to it by the supplier of the component.

Logical

Disk Boot Firmware Running Version	The version of the Disk Boot firmware currently running on the Processor Blade.
Halted State Services Firmware Running Version	The version of the HSS firmware currently running on the Processor Blade.
ISP1040 Firmware Running Version	The version of the ISP1040 firmware currently running on the Processor Blade.
Operational Status	The status of the processor blade, as seen by the OA. Possible Values: Unknown, Other, OK, Degraded, Stressed, Predictive Failure, Error, Non-Recoverable Error, Starting, Stopping, Stopped, In Service, No Contact, Lost Communication, Aborted, Dormant, Supporting Entity In Error, Completed, Power Mode, DMTF Reserved, Vendor Reserved.
iLO IPv4 Address	The IPv4 address of the iLO (Integrated Lights Out) management processor.
Power State	Indicates whether the Processor Blade is powered On or Off.

Actions

Clear Forward Progress Log

Clears the Forward Progress Log (FPL), which is more detailed than the System Event Log.

Launch iLO URL

Launches the iLO (Integrated Lights Out) management page.

Replace

Launches a documented service procedure to replace the processor blade in an Integrity NonStop Blade enclosure.

Retrieve and Clear BMC Event Log

Allows you to retrieve and save a raw Baseboard Management Controller (BMC) event log file and then clear the BMC event log.

Retrieve and Clear BMC Event Log - Formatted

Allows you to retrieve and save a formatted version of the Baseboard Management Controller (BMC) event log and then clear the BMC event log.

NOTE: With T0682 AAN and later, OSM saves a copy of each Blade Element's BMC event log to a file in \$system.zservice and clears the BMC event log daily between 1 and 2 a.m. The log file name is the format blMMMSDD, where MMM is Blade Element's module number, S is slot number, and DD is date of the month.

Retrieve Forward Progress Log

Retrieves the Forward Progress Log (FPL), which is more detailed than the System Event Log.

Processor Components

In the OSM Service Connection, each [Logical Processor](#) contains a Processor Components object to display processor attributes and – for NonStop NS14000 series and NS16000 series servers only – additional actions and attributes for the Logical Synchronization Unit (LSU) and PE(s) associated with each logical processor.

Attributes

Processor Components

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical Location

These attributes are displayed for NonStop NS14000 series and NS16000 series servers only. The values are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the LSU is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the LSU within the rack.
Locator	An optional text string assigned to further identify the physical location of the LSU. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical Location action. This attribute is displayed only if a value is specified through the action.

Processor Elements

PE (A/B/C) Blade Element Track ID	Identifies the processor element (PE) as belonging to Blade Element A, B, or C.
PE (A/B/C) LID	The local ID of the PE in the Blade Element, based on the position of the PE on the board.
PE (A/B/C) Memory Size	The memory size of the PE, in megabytes.
PE (A/B/C) Processor Model	A number assigned to each processor type to help ensure that all processors in a NonStop Blade Complex are of the same type.
PE (A/B/C) Reintegration Enable State	Indicates whether or not the PE is enabled for automatic reintegration in case of a failure. NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.

PE (A/B/C) Reintegration Progress	<p>Displayed only if a PE reintegration is in progress, this attribute displays the progress in terms of percentage complete.</p> <p>NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.</p>
PE (A/B/C) Reintegration Status	<p>Indicates the status of the PE reintegration process. Possible values include:</p> <ul style="list-style-type: none"> No current or pending operation Blade Element reset in progress Blade Element reset complete Reintegration setup in progress Reintegration copy in progress Reintegration copy complete Reintegration final phase in progress Reintegration complete Complex invalid - no current or pending operations Last operation failed Operation scheduled Settling period - no resets/reintegrations performed Reset enabled Reintegration enabled Unknown <p>NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.</p>
PE (A/B/C) State	<p>The state of the PE.</p> <p>Values: Running NSK, Halted State Services, Primitive, Primitive-Unable to Join, Dead</p>
PE (A/B/C) Stop Code	<p>Displayed only if the PE State is something other than "Running NSK." This attribute indicates why the PE is in its current state.</p>
Replacement Part Number	<p>The part number of the microprocessor assembly that was assigned in manufacturing. Use part numbers for identifying and ordering parts.</p> <p>NOTE: Displayed for NonStop NS14000 series and NS16000 series servers only.</p>

LSU Logic Board

NOTE: These attributes are displayed for NonStop NS14000 series and NS16000 series servers only.

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LSU CPLD Version	The version of the complex programmable logic device (CPLD) on the LSU Logic Board.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Rail A Power Status	Status of the LSU power supply on Rail A.
Rail B Power Status	Status of the LSU power supply on Rail B.
Serial Number	The serial number of the component assigned to it by the supplier of the component.
Slot ID	The ID of the slot in which the LSU logic board resides.

NOTE: These attributes are displayed for NonStop NS 14000 series and NS 16000 series servers only.

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Serial Number	The serial number of the component assigned to it by the supplier of the component.
Serial ZX1 I/O Link A Status	Link Status of the A cable connecting the LSU and the processor element.
Serial ZX1 I/O Link B Status	Link Status of the B cable connecting the LSU and the processor element.
Serial ZX1 I/O Link C Status	Link Status of the C cable connecting the LSU and the processor element.
Slot ID	The ID of the slot in which the LSU optics adapter resides.

Actions

These actions are available for NonStop NS 14000 series and NS 16000 series servers only. For NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC servers, there are no actions under the Processor Components object.

Disable PE Reintegration

Disables automatic reintegration of the PE (A or B or C). The automatic reintegration remains disabled for only 60 minutes after this action is performed.

Disable Serial ZX1 I/O Link

Disables the link (A or B or C) between the LSU and the processor element.

Enable PE Reintegration

Enables automatic reintegration of the PE (A or B or C) after a failure.

Enable Serial ZX1 I/O Link

Enables the link (A or B or C) between the LSU and the processor element.

Power Down LSU

This action effectively disconnects the LSU for this processor from the system and puts the LSU into low power mode, enabling it to be serviced. The LSU will only remain in low power mode for the time specified when performing the action; between 3 and 60 minutes. If more service time is required, remove the LSU optics adapter or logic board from its slot after performing the Power Down LSU action.

Reintegrate PE

Brings the PE into the same state as currently running Blade Elements.

Replace LSU

Displays the procedure for replacing LSU Logic Board and Optics Adapter components.

Reset LSU

Resets the LSU.

Set LED State

Sets these LSU LEDs to On or Off:

- Optics adapter amber LED
- Logic Board amber LED
- ServerNet X Link LED
- ServerNet Y Link LED
- Serial ZX1 I/O Link A LED
- Serial ZX1 I/O Link B LED
- Serial ZX1 I/O Link C LED

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the LSU:

- Rack Name is a user-defined name for the rack containing the LSU. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the LSU within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action will fail.
- Locator is an optional text string to help identify the physical location of the LSU. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. A system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system, while creating a physical view of your modular racks.

Stop PE

Stops PE A, B, or C (as specified).

Take Dump On Next Failure

Requests the Complex Manager AP to take the dump of the processor element if it fails. It performs a memory dump of the failed PE to the specified file before reintegrating it back into the logical processor.

Processor Switch Module

From an OSM perspective, the main component of the internal ServerNet fabric of Integrity NonStop NS5000 and NS16000 series servers. Processor switch modules provide the connections and switching logic for the processors and I/O components of the server.

Processor switch modules are initially configured using the Configure Module action in the OSM Low-Level Link, as described in the *NonStop NS-Series Hardware Installation Manual* (available in the Hardware Service and Maintenance collection of NTL).

Each processor switch module contains these components:

- A [ServerNet switch board](#), located in slot 14
- Two [power supplies](#), located in slots 15 and 18
- Two [fans](#), located in slots 16 and 17
- A [maintenance PIC](#), located in slot 1 in the back of the processor switch
- A cluster [PIC](#), located in slot 2 in the back of the processor switch
- A crosslink [PIC](#), located in slot 3 in the back of the processor switch
- I/O [PICs](#), located in slots 4-9 in the back of the processor switch
- Processor [PICs](#), located in slots 10-13 in the back of the processor switch

Location in OSM Tree:

System > Fabric Group > Internal ServerNet X Fabric > Processor Switch 100.2

System > Fabric Group > Internal ServerNet Y Fabric > Processor Switch 100.3

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

Rack Name	A user-defined name assigned to identify the rack in which the processor switch module is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the processor switch module within the rack.
Locator	An optional text string assigned to further identify the physical location of the processor switch module. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. Displays the system alarm panel (SAP) identifier for this hardware resource, as specified through the Alarm Panel Identifier option within the Set Physical Location action. This attribute is displayed only if a value is specified through the action.

Actions

Read LCD

Displays all 16 lines of the processor switch's LCD text in the Action Detail dialog box.

Rediscover

Causes OSM to refresh and reanalyze the processor switch and all subcomponents. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze

refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Replace

Launches an OSM guided procedure with step-by-step instructions for replacing the processor switch chassis or subcomponents.

Retrieve Network Connectivity Info

Displays remote IP addresses stored in the IPAUTH file of the processor switch.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the processor switch module:

- Rack Name is a user-defined name for the rack containing the processor switch. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the processor switch module within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action will fail.
- Locator is an optional text string to help identify the physical location of the processor switch module. It must contain alphanumeric characters only.
- This parameter, used for DC-powered Telco systems only, allows you to specify a system alarm panel (SAP) identifier, which is then displayed in OSM by the Alarm Panel Identifier attribute for this hardware resource. An system alarm panel (SAP) provides visual alarm indicators and relays for generating three levels of alarms to alert the customer to the severity of a hardware error in the system. By default, systems are configured with one SAP located in the CIA for the group 11 I/O enclosure. You might need to set the Alarm Panel Identifier if the system has multiple SAPs, you add equipment to a system, or you move equipment from one system to another.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system, while creating a physical view of your modular racks.

Synchronize FIR Files to Other Switches

Synchronizes the FRU information Record (FIR) files of the X and Y fabric processor switches.

Write LCD Line

Allows you to edit the text displayed by the processor switch's LCD. You can modify lines 9 through 15 with this action.

SAC (ServerNet Addressable Controller)

A LAN controller that is a component of one of these CRUs:

CRU	SACs in CRU	PIFs in SAC
CCSA	4	4
E4SA	2	2
FESA	1	1
GESA	1	1
TRSA	1	1

Location in OSM Tree: System > Group > Module > CRU > SAC

Slot Location: SACs are located on the CRUs that might be installed in slots 53 and 54 in processor enclosures (service side) or in slots 51, 52, 53, and 54 in I/O enclosures (service side).

Example: E4SA SAC \$ZZLAN.E4SA0.0

Attributes

SAC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

The Physical attributes are displayed only when the SAC is a subcomponent of a CCSA.

Device ID	The ID assigned by the device manufacturer. Example: 0x860
Manufacturer	Identifies the manufacturer of the component.
Part Number	The Part Number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Vendor ID	The manufacturer of the device. Example: 0x10E3

Logical

Automatic Boot State	Indicates whether the SAC boot firmware is automatically reloaded if it terminates abnormally: Enabled: The boot firmware is automatically reloaded. Disabled: The boot firmware is not automatically reloaded. Unknown: Automatic Boot state could not be read.
Automatic Dump State	Whether the SAC software is automatically dumped to the specified dump file if the software abends abnormally: Enabled: The software is automatically copied to a dump file. Disabled: The software is not automatically copied to a dump file. Unknown: Automatic Dump state could not be read.
Device State	The state of the component as known to the operating system on the server. Values
Download File Name	The file name of the operational firmware running on the SAC.
Download File Version	The version of the operational firmware running on the SAC.
Dump Filename	The name of the file used to store dumps of the SAC memory.
Owning Processor	The processor to which the SAC is connected. Example: 0
Processor Access List	The currently available processors that can access the SAC. Example: 0,1
SAC Type	Displayed for CCSA SACs only, displays the type of CCSA SAC (for example: SS7TE3A).

Firmware

Version	The version of the boot firmware for the SAC.
Default File Name	The name of the file to be used for a (boot) Firmware Update .
Default File Version	The version of the firmware to be used for a (boot) Firmware Update .
Compare State	The differences, if any, between the current and default boot firmware versions. Values

Actions

Abort

Terminates operation of the ServerNet Adapter ServerNet addressable controller. When the Abort action finishes, the SAC is in the Stopped state.

Firmware Update

Updates the boot firmware for the adapter SAC.

NOTE: Upon completion of the firmware update action, use the Start action on the SAC.

Responsive Test

Runs an online test that verifies the SAC is integrated with the LAN subsystem, is owned, and is in the Started state.

Start

Loads the controller operational code and starts the ServerNet addressable controller. The SAC must be in the Stopped state before you perform this action. When the Start action completes, the SAC is in the Started state.

Stop

Rather than automatically stopping the SAC (as the Abort action does), this action first warns you if the SAC is currently in use (and stops it only after you confirm).

Test Verify

Runs the power-on self-test for the SAC component of the CRU. To perform this action, the CRU must be in the Started state, and the SAC component must be in the Stopped or Diagnose state.

SAS Card (CLIM)

A subcomponent of the [CLIM](#). For the G2 and G5 CLIMs, the SAS card has only one external SAS port for connecting SAS Disk Enclosures. For the G6 and Gen8 CLIMs, the SAS card has two external SAS ports. OSM displays a "Connected Enclosures" attribute to indicate which SAS Disk Enclosure it is connected to

Location in OSM Tree: System > CLIMs > CLIM > SAS Card

Attributes

Physical

Model	The product name of the SAS card.
Serial Number	The serial number of the SAS card.

Logical

Connected Enclosures	A list of the SAS Disk Enclosure(s) to which the SAS card is attached.
----------------------	--

BIOS

Compare State	Indication of the differences, if any, between the current and default BIOS versions. Values
Default File Name	The name of the file to be used for a BIOS update.
Default File Version	The version of the firmware to be used for a BIOS update.
Version	The version of the BIOS running on the SAS card.

Firmware

Compare State	Indication of the differences, if any, between the current and default firmware versions. Values
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Version	The version of the firmware running on the SAS card.

Actions

BIOS Update

Updates the BIOS running on the SAS card.

Firmware Update

Updates the firmware running on the SAS card.

Replace

Launches a documented service procedure to replace a SAS card in a CLIM.

SAS Disk Enclosure

This object, displayed under the [SAS Disk Enclosures](#) container object in OSM, represents each SAS disk enclosure connected to a NonStop BladeSystem or supported NonStop NS-series system. A logical representation of each CLIM-attached SAS disk is displayed under the [CLIM-Attached Disks](#) object.

Each SAS Disk Enclosure object contains these subcomponents:

- [SAS Disks](#) -- a physical representation of each disk drive in the SAS disk enclosure.
- Two [SAS Fans](#)*
- Two [SAS Power Supply](#)* units.
- Two [IO Modules](#)

NOTE: For a SAS Disk Enclosure in a Telco system, the fans and power supplies are represented in OSM by a pair of [SAS Power Supply and Fan](#) objects.

Attributes

SAS Disk Enclosure

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Manufacturer	Identifies the manufacturer of the component.
Model	The model number of the SAS disk enclosure that was assigned in manufacturing.
Serial Number	The serial number of the SAS disk enclosure.

Connected SAS Card-1

SAS Card	The name of one of the two SAS cards to which this SAS disk enclosure is connected. The other is identified under the Connected SAS Card-2 attribute.
SAS Port	The port on the SAS card to which the SAS disk enclosure is connected.

Connected SAS Card-2

SAS Card	The name of one of the two SAS cards to which this SAS disk enclosure is connected. The other is identified under the Connected SAS Card-1 attribute.
SAS Port	The port on the SAS card to which the SAS disk enclosure is connected.

Logical

Fan Status	Indicates whether the status of the SAS disk enclosure fans is Fully Redundant or non-redundant.
Power Supply Status	Indicates whether the status of the SAS disk enclosure power supplies is Fully Redundant or non-redundant.
Temperature Status	Indicates whether the temperature of the SAS disk enclosure is normal or out of range.

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the SAS disk enclosure is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the SAS disk enclosure within the rack.

Firmware

Compare State	Indication of the differences, if any, between the current and default firmware versions. Values
Default File Name	The name of the file to be used for a firmware update.

Default File Version	The version of the firmware to be used for a firmware update.
Version	The version of the firmware running on the SAS disk enclosure.

Actions

Firmware Update

Updates the firmware on the SAS Disk Enclosure.

Upon successful completion, OSM now gives you the option of turning on the enclosure's LED, to help you identify the enclosure for the purpose of power cycling it to complete the firmware update process

Replace

Launches a documented service procedure to replace the SAS disk enclosure in a NonStop BladeSystem or supported NonStop NS-series system.

Set LED State

Turns the LED on the SAS disk enclosure on or off.

SAS Disk Enclosures

This object contains each [SAS Disk Enclosure](#) connected to a NonStop BladeSystem or supported NonStop NS-series system.

Attributes

None.

Actions

None.

SCSI Controller

A controller that manages devices using the Small Computer System Interface (SCSI) protocol. This SCSI controller is a component of I/O Multifunction ([IOMF2](#)) CRUs.

Location in OSM Tree: System > Group > Module > IOMF2 > SCSI Controller

Slot Location: SCSI controllers are located on IOMF2 CRUs in slots 50 and 55 of I/O enclosures.

Example: SCSI Controller (1.1.55.1)

Attributes

SCSI Controller

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

SCSI ID	The ID to which the device answers on the SCSI bus: 4 or 5: Tape devices 6 or 7: Controllers 8 and 9: SCSI extenders/FC converters
---------	---

	The remaining IDs are for the device on the SCSI bus.
SCSI Bus Number	The bus to which the device is attached: Bus 1 or 2: Internal device Bus 3: External device

Actions

Responsive Test

Verifies that the component is installed and responding.

ServerNet Interface Card (Blade)

A processor switch plug-in card (PIC) used to provide internal ServerNet connections for the Blade. In the OSM Service Connection, this object is displayed as a subcomponent of:

- [Blade Element](#) object for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, and NS3000AC servers.
Location in OSM Tree: System > Blade Complex > Blade Element > ServerNet Interface Card
- [Processor Blade](#) object for Integrity NonStop BladeSystems.
Location in OSM Tree: System > Enclosure > Processor Blade > ServerNet Interface Card

Attributes

ServerNet Interface Card

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. Displayed only for Integrity NonStop NS1000, NS1200, NS2000 series, NS5000, and NS3000AC servers.
-------------	--

Actions

Replace

Launches a documented service procedure to replace the ServerNet Interface Card in a [Processor Blade](#).

NOTE: Displayed only for (J-series) NonStop BladeSystems; not applicable for NonStop NS-series servers.

ServerNet Interface Card (CLIM)

A subcomponent of the [CLIM](#).

Location in OSM Tree: System > CLIMs > CLIM > ServerNet Interface Card

Attributes

ServerNet Interface Card

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Model	The product name of the ServerNet interface card.
-------	---

Actions

Replace

Launches a documented service procedure to replace a ServerNet interface card in a CLIM.

ServerNet PIC

A processor switch plug-in card (PIC) used for internal ServerNet connections. ServerNet PICs are installed in slots 2 through 13 of the processor switch. Each PIC contains two to four [ports](#). Depending on the needs of your system, some slots might not have PICs installed.

- Slot 2 contains a cluster PIC if your system is part of a ServerNet cluster.
- Slot 3 contains a crosslink PIC that connects the X-fabric and Y-fabric processor switches.
- Slots 4 through 9 contain I/O PICs that connect to an IOAM enclosure or Nonstop S-series IOMF2 enclosures.
- Slots 10 through 13 contain processor PICs that connect to the processors.

Attributes

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether or not the power supply's amber LED is lit. This state is determined by the Set LED State action. Value: On or Off
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Indicates whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Type	Identifies the type of ServerNet PIC. Value: Quad Single Mode Fibre, Dual Single Mode Fibre, Quad Multi Mode Fibre, Dual Multi Mode Fibre, Crosslink, LoopBack, Maintenance

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Actions

Enable ServerNet Port

Enables the specified ServerNet port on this PIC. Perform this action only as directed by OSM alarm repair actions. Each PIC contains two to four ports.

Parameter: Port Number

Power Off

Removes power to the PIC.

When a crosslink PIC is powered off or removed, the loss of ServerNet cluster traffic on a single fabric is expected. Other nodes in the cluster continue to communicate over that fabric. ServerNet cluster traffic on the lost fabric is automatically restored when the crosslink PIC is reinserted or powered on.

Power On

Restores power to the PIC.

Replace

Launches the guided procedure to replace a ServerNet PIC in a processor switch.

Set LED State

Turns on or off the amber LED located on the PIC. The current state is indicated by the [LED State](#) attribute.

ServerNet Port

In OSM, this object represents ports on:

- ServerNet PICs located within Processor Switches
- ServerNet Switch Boards located within IOAM Enclosures
- 4-Port ServerNet Extenders (4PSEs) located only in HP Integrity NonStop NonStop NS14000 or NonStop NS1000 systems containing IOAMs
- [VIO Logic Board](#) located in systems containing VIO enclosures.

OSM displays five ports under a VIO Logic Board – ports 1 through 4 provide connectivity to processors 0 through 3; port 5 represents the crosslink connectivity to the VIO enclosure on the opposite fabric.

- [Optical Extender PICs](#) located only in HP Integrity NonStop NonStop NS14000 series, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS1200, or NonStop NS1000 systems containing VIO enclosures.

In slot 2, an extender PIC can be used for connectivity to additional processors, with ports 1 through 4 corresponding to processors 4 through 7.

In slot 5 (Integrity NonStop NS14000 series servers only), an extender PIC can be used for ServerNet cluster connectivity. Port 1 is where the cable from the cluster switch is physically connected to. For more information about ServerNet cluster connectivity for VIO enclosures, see the *ServerNet Cluster Supplement for NS-Series*.

- ServerNet switches located in Enclosures in NonStop BladeSystems. Under these port objects, OSM displays Fiber objects.

Attributes

Logical

Connector Type	Values include: QSFP, POP4, SFP, Snap12
Link Status	Displays the status of this port. Values: Disabled, Neighbor Check In Progress, Enabled
Neighbor Check Status	Displays the status of the port to which this port is connected. Values: OK, Fabric connection error, PIC connection error, Port connection error, Domain connection error, System connection error, Timeout error, Unknown

NOTE: In processor switches, these attributes are not displayed for Port 1 of the crosslink PIC located in slot 3.

Actions

None.

ServerNet Switch (Blade Enclosure)

There are two ServerNet switches in each [Enclosure](#) of a NonStop BladeSystem. Under each switch object, OSM displays [Port](#) objects.

OSM software communicates with an internal part of the switch known as the Maintenance Entity (ME) by a connection established through the [Maintenance Switch](#).

Location in OSM Tree: System > Enclosure > ServerNet Switch

Attributes

ServerNet Switch

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing.
Product Name	The product name of the component as assigned by the manufacturer.
Replacement Part Number	The replacement part number of the component.
Serial Number	The serial number of the component assigned to it by the supplier of the component.

Logical

IPv4 Address	The IPv4 address of the ServerNet switch.
Operational Status	The status of the ServerNet switch, as seen by the Onboard Administrator (OA).
Time of Last Reset	The date and time of the last hard or soft reset of the ServerNet Switch Board.

ME FPGA

Version	The VPROC of the ME FPGA (Field Programmable Gate Array) image currently loaded on the switch.
Default File Name	The full path name of the default ME FPGA file on the server.
Default File Version	The version of the ME FPGA image in the default FPGA file.
Compare State	The differences, if any, between the current and default ME FPGA versions. Values

ME Firmware

Version	The version of the ME firmware running on the switch.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Compare State	The differences, if any, between the current and default firmware versions. Values

Actions

Dump Memory

Dumps a snapshot of the ServerNet Switch Board's memory to a file in \$SYSTEM.ZSERVICE.

You can view the filename in the Action Detail dialog box for this action.

The filename convention is *ZMmmmssn*, where:

mmm = group (enclosure) number

ss = module number

n = version number (incremented for subsequent versions of the same *ZMmmmss* snapshot files)

Example: ZM100021: snapshot file taken of ServerNet Switch in group (enclosure) 100, module 02, version number 1.

Hard Reset

Resets the ServerNet Switch hardware and the routing tables.

Launch Switch URL

Launches the management URL for the ServerNet switch.

ME FPGA Update

Allows you to update the FPGA code file for the Maintenance Entity (ME) of the ServerNet Switch.

NOTE: Because the hard reset required to complete an FPGA update disrupts a ServerNet fabric, you should perform a [Check Storage Dependence on ServerNet Fabric](#) action to make sure it is safe before proceeding with the FPGA update. Then, update the ServerNet switch boards on a single fabric at a time and wait at least 5 minutes after completion before checking storage dependence and updating the switch boards on the other fabric.

ME Firmware Update

Allows you to update the firmware file for the Maintenance Entity (ME) of the ServerNet Switch.

Replace

Launches the service procedure to replace the ServerNet switch in a Blade enclosure.

Soft Reset

Reinitializes the firmware without affecting the ServerNet Switch hardware or the routing tables.

Synchronize FIR Files to Other Switches

Synchronizes the FRU information record (FIR) files of the X and Y fabric ServerNet switches. The files will be synchronized from the switch on which this action is executed to the other switch.

ServerNet Switch Board

A component of both the [IOAM](#) and [Processor Switch](#), the ServerNet Switch Board provides ServerNet connectivity between processors, ServerNet adapters, and attached hardware devices. OSM software communicates with an internal part of the switch known as the Maintenance Entity (ME) by a connection established through the [Maintenance Switch](#).

While always named ServerNet Switch Board in the OSM tree pane, the Multi-Resource Actions dialog box uses unique names to differentiate between the different types:

- A ServerNet Switch Board in a processor switch module is displayed as a Processor ServerNet Switch Board.
- An IOAM ServerNet Switch Board in an HP Integrity NonStop NS16000 series server is displayed as a ServerNet Switch Board.
- An IOAM ServerNet Switch Board in an HP Integrity NonStop NS14000 or NS1000 server (which has no processor switches), is displayed as an IO/Switch Board.

Location in OSM Tree:

In an IOAM: System > Group > IOAM Enclosure > IOAM > ServerNet Switch Board

Examples:

- In an Integrity NonStop NS16000 series server: ServerNet Switch Board (110.2.14)
- In an Integrity NonStop NS14000 or NS1000 server: ServerNet Switch Board (100.2.14)

In a Processor Switch: System > Fabric Group > Internal ServerNet Fabric > Processor Switch > ServerNet Switch Board

Example: ServerNet Switch Board (110.2.14)

Attributes

ServerNet Switch Board

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether the ServerNet Switch Board LED is on or off.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Time of Last Reset	The date and time of the last hard or soft reset of the ServerNet Switch Board.
Fabric Side	This attribute is displayed only within the Multi-Resource Actions dialog box, to indicate whether the ServerNet Switch Board is on the X or Y fabric.

ME FPGA

Version	The VPROC of the ME FPGA (Field Programmable Gate Array) image currently loaded on the switch logic board.
Default File Name	The full path name of the default ME FPGA file on the server.
Default File Version	The version of the ME FPGA image in the default FPGA file.
Compare State	The differences, if any, between the current and default ME FPGA versions. Values

ME Firmware

Version	The version of the ME firmware running on the switch board.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	The differences, if any, between the current and default firmware versions. Values

Actions

Dump Memory

Dumps a snapshot of the ServerNet Switch Board's logic board memory to a file in \$SYSTEM.ZSERVICE.

You can view the filename in the Action Detail dialog box for this action.

The filename convention is ZMmmmssn, where:

mmm = group number

ss = module number

n = version number (incremented for subsequent versions of the same ZMmmmss snapshot files)

Example: ZM100023: snapshot file taken of ServerNet Switch Board in group 100, module 02, version number 3.

Hard Reset

Resets the ServerNet Switch Board hardware and the routing tables.

ME FPGA Update

Allows you to update the FPGA code file for the Maintenance Entity (ME) of the ServerNet Switch Board.

NOTE: Because the hard reset required to complete an FPGA update disrupts a ServerNet fabric, you should perform a [Check Storage Dependence on ServerNet Fabric](#) action to make sure it is safe before proceeding with the FPGA update. Then, update the ServerNet switch boards on a single fabric at a time and wait at least 5 minutes after completion before checking storage dependence and updating the switch boards on the other fabric.

ME Firmware Update

Allows you to update the firmware file for the Maintenance Entity (ME) of the ServerNet Switch Board.

Power Cycle

Power cycles the ServerNet Switch Board.

Replace

Launches the guided procedure to replace a ServerNet switch board in an IOAM or processor switch.

NOTE: For an HP Integrity NonStop NS14000 or NS1000 system, the Replace action launches a documented service procedure describing how to replace a ServerNet Switch Board unique to that type of system.

Set LED State

Turns the ServerNet Switch Board LED on or off.

Soft Reset

Reinitializes the firmware without affecting the ServerNet Switch Board hardware or the routing tables.

Service Processor (SP)

The service processor (SP) controls environmental and maintenance functions and acts as the master of the serial maintenance bus (SMB). The service processor is a physical component of [IOMF2](#) CRUs.

Location in OSM Tree: System > Group > Module > IOMF2 > SP

Slot Location: Service processors are located in slots 50 and 55 of I/O enclosures (service side).

Example: SP (1.1.50)

Attributes

SP

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Current Topology	The maximum processor configuration for the service processor. Values
Device State	The state of the service processor: Active (Primary): This is the active SP and it is available. Active (Secondary): This is not the active SP, but it is available. Firmware Update Mode: An SP firmware update is in progress. In Test: Temporary state during power-on self-test. Initializing: Temporary state during startup. SP Stopped Responding to Peer:
IPv4 Address	The IPv4 address of the service processor.

Master SP	Indicates whether this service processor is the master service processor on the system: Indicates whether this service processor is the master service processor on the system. The value will always be False on a legacy IOMF2 SP in an Integrity NonStop NS-series server.
Running Image Source	Indicates whether the SP firmware was loaded from its own (local), the peer's, or the backup flash memory.
Stored Topology	The maximum processor configuration for the service processor that is set the next time the system or enclosure is powered on. Values
Time of Last Reset	The date and time that the service processor was last reset.
Fabric Side	This attribute is displayed only within the Multi-Resource Actions dialog box, to indicate whether the SP is on the X or Y ServerNet fabric.

SP Firmware

Version	The VPROC of the firmware currently loaded on the service processor.
Default File Name	The name of the file to be used for the service processor firmware update. (SPCODE9)
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	The differences, if any, between the current and default firmware versions. Values

SCSI Boot Code Firmware

These attributes are displayed only for SPs located in PMF or PMF2 CRUs; not for those in IOMF or IOMF2 CRUs.

Version	The version of the firmware running on the SCSI controller on the PMF CRU that contains the service processor.
Default File Name	The name of the file to be used for the SCSI Boot Code firmware update.
Default File Version	The version of the firmware to be used for the SCSI Boot Code firmware update.
Compare State	The differences, if any, between the current and default firmware versions. Values

Processor Boot Millicode Firmware

These attributes are displayed only for SPs located in PMF or PMF2 CRUs; not for those in IOMF or IOMF2 CRUs.

Version	The version of the firmware on the processor on the same PMF CRU with this service processor.
Default File Name	The name of the file to be used for the Processor Boot Millicode firmware update. (CPUCODE9)
Default File Version	The version of the firmware to be used for the Processor Boot Millicode firmware update.
Compare State	The differences, if any, between the current and default firmware versions. Values

Actions

Reset

Causes the service processor (SP) to reload the service processor operating image from the FLASH PROM.

If the CLCI and CNSL (console) sessions are running through an SP that is reset, the session windows stop responding, and you must switch to the other paired SP by specifying the appropriate IP addresses.

When you reset a master service processor (MSP), any LAN client connections to that MSP are terminated and must be reconnected by the client.

Responsive Test

Verifies that the component is connected and responding.

SP Firmware Update

Updates the firmware for a single service processor (SP).

Optional Parameter: File Name – the name of the firmware file.

Syntax: \$volume.subvolume

Default value: \$SYSTEM.SYSnn

Smart Array Controller (CLIM)

A subcomponent of G6 and Gen8 [CLIMs](#).

Location in OSM Tree: System > CLIMs > CLIM > Smart Array Controller

Attributes

Smart Array Controller

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the Smart Array Controller as known to the operating system on the server. Possible values include: OK and Fault.
--------------	--

Physical

Model	The model number of the Smart Array Controller that was assigned in manufacturing.
Serial Number	The serial number of the Smart Array Controller.

Firmware

Compare State	Indication of the differences, if any, between the current and default Smart Array Controller firmware versions. Values
Default File Name	The name of the file to be used for a Smart Array Controller firmware update.

Default File Version	The version of the firmware to be used for a Smart Array Controller firmware update.
Version	The version of the Smart Array Controller firmware running on the CLIM.

Actions

Firmware Update

Updates the firmware running on the Smart Array Controller. Upon completion, OSM offers to reboot the CLIM, in order for the CLIM to start using the updated firmware.

SNDA (ServerNet/DA)

The ServerNet/DA CRU (customer-replaceable unit) is an adapter that allows external storage devices to be connected to servers. The external storage devices are physically connected to either Fiber SACs ([FSAC](#)) or SCSI SACs ([SSAC](#)) mounted on the ServerNet/DA CRU.

Location in OSM Tree: System > Group > Module > SNDA

Slot Location: ServerNet/DA CRUs can be located in 51, 52, 53, and 54 in I/O enclosures (service side).

Example: SNDA (12.1.54)

Attributes

SNDA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Storage ASIC

Initialization State	The status of the storage ASIC in the CRU. Values: Initialized, Not Initialized, Unknown
----------------------	--

Actions

Replace

Launches the Replace SNDA guided procedure, which provides step-by-step instructions for replacing the ServerNet/DA CRU.

Storage ASIC Initialization Test

Prompts the storage subsystem manager process (\$ZZSTO) to initialize the storage ASIC in the CRU. If initialization fails, an alarm is generated.

This action is triggered automatically when a new CRU is inserted while OSM is running or when an SCF STATUS ADAPTER command is issued. If a CRU is inserted while OSM is not running, perform this action after logging on to the OSM Service Connection.

Test Verify

Performs basic tests on the CRU. You can perform this action when the CRU is online.

SSAC (SCSI SAC)

The SCSI SAC (ServerNet addressable controller) is a SCSI plug-in card mounted on these devices:

- I/O multifunction (IOMF2) 2 CRU (external SCSI controller, SAC 3)
- ServerNet/DA CRU (There can be up to four SCSI SACs on each ServerNet/DA CRU.)

SCSI SACs are used for connecting external SCSI devices such as tape drives.

Location in OSM Tree: System > Group > Module > IOMF2 > SSAC

Example: SSAC (1.1.50.3)

Attributes

SSAC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Type	The type of CRU this SAC is connected to. values: SSAC, FSAC, SCSI
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Logical

Configured Type	The type of device supported by this SAC. Values: Disk, Tape, SCSI Controller, Not Configured, Unknown
-----------------	--

Actions

Responsive Test

Verifies that the component is connected and responding.

Storage Router

This object represents one of these resources:

SCSI Extender

A pair of SCSI extenders (one SCSI-to-Fiber extender and one Fiber-to-SCSI extender) can be used to increase the distance between the host system and any of these devices to a maximum of 10 kilometers:

- 9840 cartridge tape drive
- T525x Super DLT tape drive
- 5242 DAT72 tape drive (all models)
- Virtual tape subsystems (all models)
- N152x LTO tape drives (all models)

SCSI-to-Fiber Converter

A Fibre Channel (scsi to fiber) converter is used to connect the following tape drives:

- CT9840FC
- CT9841FC

to the host system through a SCSI SAC on one of these supported CRUs:

- IOMF2
- ServerNet/DA

Location in OSM Tree: System > Tape Collection > Tape Drive > Storage Router

Example: Storage Router \$EXT8

Attributes

Storage Router

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Router Type	The type of router. Values: SCSI Extender or SCSI-to-Fiber Converter
Logical Device Number	The number assigned to the router by the file system.
Communication State	Whether the resource is communicating to the host system. Values: Communicating, Not Communicating, Unknown
Product ID	A unique number that identifies the product as a SCSI Extender (2 models) or SCSI to Fiber Converter. Otherwise, Unknown is shown.
Device State	The state of the component as known to the operating system (open scsi process) on the server. Values
Configured Controller Location	The location of the configured SCSI controller. Example: PMF.SAC-3.GRP-1.MOD-1.SLOT-55

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. This is not the spare part number.
-------------	--

Process Pair

Configured Processors	The 2 processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296
Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285

SCSI Interface

SCSI ID	An identification number assigned to the device when configured. 8: SCSI-to-Fiber extender / SCSI to Fiber Converter 9: Fiber-to-SCSI extender
SCSI Controller	The number that identifies the SCSI controller that manages the storage router. If this attribute is missing, it is because the SCSI Controller has been removed from the system. Example: SSAC (1.1.50.3)

Actions

Responsive Test

Verifies that the resource is configured and responding.

Switch Process Pair

Switches processors of the primary and backup tape I/O processes

SWAN / SWAN2

The ServerNet wide area network (SWAN) concentrator CRU is an external communications device that connects to a system through dual Ethernet ports. It supports both synchronous and asynchronous protocols over a variety of electrical interfaces. The SWAN CRU object displayed by OSM can be either a SWAN or SWAN 2 CRU. To distinguish between them, look at their subcomponents.

Each SWAN CRU contains up to three [CLIPs](#), each of which contains two [SWAN Paths](#) and two [WAN Lines](#), giving each SWAN CRU as many as six WAN ports.

Each SWAN 2 CRU contains these subcomponents:

- Up to six [SWAN 2 CLIPs](#), each of which contains two SWAN Paths and two WAN Lines, giving each SWAN 2 CRU as many as twelve WAN ports
- Two [LAN Logic Board CRUs](#)
- Two [Fan CRUs](#)
- Two [Power Supply CRUs](#)
- One [Battery](#)

Location in OSM Tree: System > SWAN Collection > SWAN [or SWAN2]

Slot Location: WAN CRUs are external to the enclosures.

Example: SWAN2 \$ZZWAN.#SWAN2

Attributes

SWAN \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Logical

Adapter Type	The type of SWAN concentrator. Values: Synchronous or Firmware Controlled
Adapter State	The state of the SWAN concentrator CRU as known to the operating system. Values: Started, Stopped, Starting, Stopping, Aborted, Aborting, Out Of Service, Unknown, Not Configured
Primary Host IPv4 Address	The primary host IPv4 address configured for the SWAN concentrator.
Alternate Host IPv4 Address	The alternate host IPv4 address configured for the SWAN concentrator.
Primary TCP/IP Process	The primary TCP/IP process configured for the SWAN concentrator. Example: \$ZTCP2
Alternate TCP/IP Process	The alternate TCP/IP process configured for the SWAN concentrator. Example: \$ZTCP1
Primary Subnet Mask	The name of the subnet mask configured for the primary host IP address for the SWAN concentrator. Example: 255.255.255.0
Alternate Subnet Mask	The name of the subnet mask configured for the Alternate host IP address for the SWAN concentrator. Example: 255.255.255.0
Primary Subnet Name	The name of the subnet on the primary TCP/IP process that supports the SWAN concentrator. Format: TCP/IP process name.subnet name Example: \$ZTCP1.#SN1
Alternate Subnet Name	The name of the subnet on the alternate TCP/IP process that supports the SWAN concentrator. Format: TCP/IP process name.subnet name Example: \$ZTCP3.#SN1
Primary Gateway IPv4 Address	The primary gateway IPv4 address configured for the SWAN concentrator. Example: 192.168.10.30
Alternate Gateway IPv4 Address	The alternate gateway IPv4 address configured for the SWAN concentrator. Example: 192.168.11.30

Primary Host Connection

Host Connection Point	If the primary path of this SWAN concentrator is connected to a CLIM, this attribute is the name of the primary CLIM. If the primary path of this SWAN concentrator is connected to a PIF, this attribute is the location of the SLSA adapter containing the primary PIF. Format: \$ZZCIP.CLIM_Name, (Group, Module, Slot) Example: \$ZZCIP.C1002581, (110, 2, 4)
Host Interface	If the primary path of this SWAN concentrator is connected to a CLIM, this attribute is the name of the Ethernet interface in the primary CLIM to which the SWAN concentrator is connected. If the primary path of this SWAN concentrator is connected to a PIF, this attribute is the name of the LIF corresponding to the primary PIF to which the SWAN concentrator is connected. Format: CLIM_Name.Interface_Name, LIF \$ZZLAN.LIF_Name Example: C1002581.eth2, LIF \$ZZLAN.LANA

Alternate Host Connection

Host Connection Point	If the alternate path of this SWAN concentrator is connected to a CLIM, this attribute is the name of the alternate CLIM. If the alternate path of this SWAN concentrator is connected to a PIF, this attribute is the location of the SLSA adapter containing the alternate PIF. Format: \$ZZCIP.CLIM_Name, (Group, Module, Slot) Example: \$ZZCIP.C1002582, (110, 2, 4)
Host Interface	If the alternate path of this SWAN concentrator is connected to a CLIM, this attribute is the name of the Ethernet interface in the alternate CLIM to which the SWAN concentrator is connected. If the alternate path of this SWAN concentrator is connected to a PIF, this attribute is the name of the LIF corresponding to the alternate PIF to which the SWAN concentrator is connected. Format: CLIM_Name.Interface_Name, LIF \$ZZLAN.LIF_Name Example: C1002582.eth2, LIF \$ZZLAN.LANB

Actions

Start

Starts the SWAN concentrator and its associated CLIPs. When the Start action completes, the SWAN concentrator and its associated CLIPs are in the Started state.

In a multisystem configuration, this action also causes the current system to take control of the associated CLIPs. If any of the CLIPs are currently controlled by another system, that system loses control of those CLIPs.

Stop

Terminates operation of the SWAN concentrator and all associated SWAN CLIPs. When the Stop action completes, the SWAN CRU and associated SWAN CLIPs are in the Stopped state.

Verify Logical Configuration

Verifies that the SWAN Concentrator CRU is properly configured. If not, an Incorrect Logical Configuration alarm is generated on the CRU.

SWAN Battery

A subcomponent of the [SWAN 2](#) CRU that provides backup power for 30 seconds in the event of a power outage.

Location in OSM Tree: System > SWAN Collection > Battery

Example: Battery \$ZZWAN.#SWAN2.BAT

Attributes

Battery \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Charge Status	The charge status of the SWAN 2 battery. Values: Charging, Critical (Discharging), Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

None.

SWAN CLIP

A communications line interface processor (CLIP) is a component of a [SWAN](#) or [SWAN 2](#) CRU. The CLIP provides a link-level protocol and a software interface to the host.

Each SWAN concentrator contains up to three CLIPs, and each CLIP has two [WAN Lines](#) and two [SWAN Paths](#).

Each SWAN 2 CRU contains up to six SWAN 2 CLIPs, and each CLIP has two WAN Lines and two SWAN Paths.

Location in OSM Tree: System > SWAN Collection > SWAN > CLIP

Slot Location: CLIPs are external to the enclosures.

Example: CLIP \$ZZWAN.# SWAN2.2

Attributes

CLIP \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	--

Physical

The Physical attributes are displayed for SWAN 2 CLIPs only.

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Firmware

Version	The version of the firmware on the concentrator communications line interface processor (CLIP) of the ServerNet wide area network (SWAN).
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	The differences, if any, between the current and default firmware versions. Values

Actions

Firmware Update

Updates the firmware on the ServerNet wide area network (SWAN) concentrator communications line interface processor (CLIP).

Optional Parameter: File Name of the firmware file.

There is no SWAN Fast Firmware Update guided procedure in OSM because you can use the [Multi-Resource Actions](#) to stop, update, and restart any or all SWAN CLIPs on your system simultaneously.

Start

Starts the SWAN CLIP. When the Start action completes, the SWAN CLIP is in the Started state.

In a multisystem configuration, this action also causes the current system to take control of the CLIP. If the CLIP is currently controlled by another system, that system loses control of the CLIP.

Stop

Terminates operation of the SWAN CLIP. When the Stop action completes, the SWAN CLIP is in the Stopped state.

Test Backup Path Access

Tests two-way access to the communications line interface processor (CLIP) using the alternate address.

Test Basic Online

Runs an online test to determine if the CLIP is functional, and checks that both the access paths are available.

Test Full Path Access

Tests two-way access to the communications line interface processor (CLIP) using both the primary and alternate addresses.

Test Primary Path Access

Tests two-way access to the communications line interface processor (CLIP) using the primary address

Test Verify

Runs the power-on self-test for the CLIP. The FAULT LED on the CLIP flashes during the test. If the test passes, the FAULT LED goes off. If the test fails, the FAULT LED remains on continuously.

SWAN Collection

When one or more [SWAN](#) or [SWAN 2](#) concentrator CRUs are connected to a system, a SWAN Collection object appears in both the tree pane and the overview pane of the OSM Service Connection. In both panes, this object displays an alarm or yellow icon if alarms or degraded conditions exist on any of the individual SWAN CRUs contained within. You can expand the SWAN Collection icon in the tree pane (but not in the overview pane) to select and monitor individual SWAN CRUs and their subcomponents.

Location in OSM Tree: Under System

Example: SWAN Collection

Attributes

None.

Actions

None.

SWAN FAN

Each SWAN 2 CRU has two customer-replaceable fan subcomponents.

Location in OSM Tree: System > SWAN Collection > SWAN > Fan

Example: Fan \$ZZWAN.#SWAN2.FAN1

Attributes

Fan \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	---

Actions

None.

SWAN LAN Logic Board (LANLB)

Each SWAN 2 CRU has two customer-replaceable LAN logic board subcomponents.

Location in OSM Tree: System > SWAN Collection > SWAN > LANLB

Example: LAN LB \$ZZWAN.#SWAN2.LAN1

Attributes

LAN LB \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Logical

Link State	The status of the Ethernet link. Values: Up, Down, Not Available
Duplex Mode	The duplex mode of the connection between the logic board and the router. Values: Half Duplex, Full Duplex, Not Available
Maximum Speed	The maximum speed of the connection between the logic board and the router. Values: 10Mbps, 100Mbps, Not Available
Board State	The operational status of the SWAN 2 LAN logic board CRU. Values: OK, Fault, Not Available

Actions

None.

SWAN Line

A subcomponent of [SWAN CLIPs](#) and SWAN 2 CLIPs. Every CLIP has two lines, which represent the ports on the CLIP.

Location in OSM Tree: System > SWAN Collection > SWAN > CLIP > Line

Example: Line \$ZZWAN.#SWAN2.1.0

Attributes

Line \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device Name	The name of the WAN device associated with the line. Example: \$TP6S1 If no device is configured, "FREE" is shown.
DLC Task Name	The name of the data link control (DLC) task associated with the line. Format: adapter.name.clip.number.DLC line number

	Example: \$ZZWAN.#D08XE5.1.DLC0
DLC Task State	The state of the data link control (DLC) task associated with the line as known to the operating system. Values: Starting, Started, Stopped, Unknown, and Indeterminate (CLIP is inaccessible).

Actions

External Loopback Test

Performs the external loopback firmware diagnostic test.

Start DLC Task

Starts the data link control (DLC) task associated with the SWAN Line. When the Start action completes, the task is in the Started State.

Stop DLC Task

Stops the data link control (DLC) task associated with the SWAN Line. When the Stop action completes, the task is in the Stopped State. Device objects already using the task are not affected by this action, but subsequent attempts to download tasks will fail.

SWAN Path

A subcomponent of [SWAN CLIPs](#) and SWAN 2 CLIPs. Every CLIP has two paths, path A and path B. These paths represent the two Ethernet interfaces on the SWAN concentrator.

Location in OSM Tree: System > SWAN Collection > SWAN > CLIP > Path

Example: PATH \$ZZWAN.#SWAN2.1.B

Attributes

PATH \$ZZWAN

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

MAC Address	The media access control (MAC) address of the SWAN Path.
IPv4 Address	The IPv4 address configured for the SWAN Path.
Path State	The state of the SWAN Path as known to the operating system. Values: Started, Stopped

Actions

Start

Starts the SWAN Path. When the Start action completes, the SWAN Path is in the Started state.

Stop

Terminates operation of the SWAN Path. When the Stop action completes, the SWAN Path is in the Stopped state.

Verify Logical Configuration

Verifies that the SWAN Path is properly configured. If not, an Incorrect Logical Configuration alarm is generated on the SWAN Path.

SWAN (Power Supply)

Each SWAN 2 CRU has two customer-replaceable power supply subcomponents.

Location in OSM Tree: System > SWAN Collection > SWAN > Power Supply

Example: Power Supply \$ZZWAN.#SWAN2.PS2

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.

Logical

Device State	The state of the component as known to the operating system on the server. Values
--------------	---

Actions

None.

System

A system is made up of all the hardware components, software, and firmware that are managed by a single operating system. Internal hardware components are housed in enclosures and are arranged in groups, modules, and slots. User-replaceable components are known as customer-replaceable units (CRUs). Components that must be replaced by your service provider are known as field-replaceable units (FRUs). Both CRUs and FRUs can contain subcomponents.

Location in OSM Tree: Located at the top level

Example: System \STARZ

Attributes

System

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Current Topology	The maximum processor configuration for the service processor. Values
Power Regulator Management Supported	Displayed only for NonStop BladeSystems, this attribute will show a value of True for an NB54000 series BladeSystem running a NonStop RVU that supports HP Power Regulator management; in all other cases, the value will be False.
Power Regulator Management Status	Displayed only the value of the Power Regulator Management Supported attribute is True. When displayed, the possible values for this attribute include: <ul style="list-style-type: none">• Enabled – displayed when Power Regulator management has been enabled through the Enable/Disable Blade Power Regulator Management action.• Disabled – displayed when Power Regulator management has been disabled through the Enable/Disable Blade Power Regulator Management action.• Not Supported – displayed whenever the Power Regulator Management Supported attribute is False.• Unknown – displayed when the Power Regulator Management Supported attribute is True, but the OSM action to Enable/Disable Blade Power Regulator Management has never been issued.
Stored Topology	The maximum processor configuration for the service processor that will be set the next time the system or enclosure is powered on. Values
System Serial Number	A unique identification number assigned to a server when it is manufactured. This number is passed automatically to your service provider when OSM dials out an incident report. Your service provider tracks systems using system serial numbers.
System Type	Indicates whether the system is a standard "Commercial" (AC-powered) or "Central Office" (DC-powered) system.

Operating System

Version	The release version update of the operating system that is running on the server. Example: H06.03 Other values that might be displayed for Operating System Version are Not Running and Halted.
---------	--

Data Collection Services

Automatic Data Collection State	Indicates whether automatic data collection for failed system resources is enabled or disabled. To change this attribute state, use the Enable/Disable Automation of Data Collection action.
Diagnostic Data Collection Volume	Indicates the volume in which automatic or manual data collection will take place. This volume is assigned by using the Set Data Collection Volume action.
Days to Persist Collected Diagnostic Data	Indicates the number of days that collected hardware failure data (collected either automatically or by the Collect Diagnostic Data action) is retained on the system before being deleted.

System Load Configuration

Configuration Name	Displays the name of an alternate system load configuration, as specified through the Save As System Load Configuration action (located under the Disk , FC Disk , and CLIM-Attached Disk objects in the OSM Service
--------------------	--

	<p>Connection). You can specify up to four such alternate system disks; each one is displayed in the system attributes (under a separate System Load Configuration heading), and can be selected from the Configuration menu of the System Load dialog box in the OSM Low-Level Link.</p> <p>These configurations can be deleted by the system-level Delete System Load Configuration action.</p> <p>NOTE: With OSM Low-Level Link T0633 AAQ and later, you can also save system configuration files on the system console. Those saved configurations are not displayed as attributes values in the OSM Service Connection, but can be used during the system load operations in the Low-Level Link. For more information, see the OSM Low-Level Link online help.</p>
Disk Name	The name of this alternate system disk, as configured in SCF.

Incident Report Configuration

Problem Incident Report Creation State	<p>Indicates whether or not OSM's ability to create Problem Incident Reports has been suppressed. This suppression is accomplished by the Suppress Problem Incident Report Creation action and is desirable to stop dial-out of known problems, such as those that may occur during CRU replacements.</p> <p>Values: Suppressed, Unsuppressed</p>
--	--

Actions

Add Node to ServerNet Cluster

Launches a guided procedure that adds the local system to a ServerNet Cluster or [BladeCluster](#). This procedure is also used to configure or display information for Expand-over-ServerNet line handlers.

NOTE: This action is not applicable for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, or NS3000AC servers.

Bring Up and Balance Storage Paths

Launches a guided procedure to help recover from ServerNet disruption to storage paths.

Check DHCP and DNS Server Status

Invokes checks to determine whether DHCP, DNS, and TFTP servers are running.

OSM also automatically performs periodic checking of these services. Performed every 24 hours by default, the frequency is configurable through an OSMCONF setting. For more information on OSMCONF settings, see the *OSM Configuration Guide*.

Check Storage Dependence on ServerNet Fabric

Launches a guided procedure to determine whether system components are dependent upon a particular ServerNet fabric. This is recommended as a pre-check before performing service procedures that disrupt ServerNet traffic on one fabric, such as replacing a P-switch (or ServerNet Switch Board, for systems without P-switches), updating ME FPGA, or performing a Power Cycle or Hard Reset action.

Clear External BladeCluster Configuration

This action clears the existing cluster configuration on the system.

Collect Diagnostic Data

This action collects diagnostic data for your system. Upon performing the action, you are prompted to specify date and time parameters. Based on the date and time specified:

- Diagnostic events are collected for a period of 12 hours (configurable through OSMCONF file) before and three hours after the specified date and time.
- Diagnostic Data files, such as ZZAxxxx, ZZSNxxxx, and ZZPSxxxx, are collected for a period of three hours starting from the specified date and time.

The volume in which this diagnostic data is collected is specified by the [Set Data Collection Volume](#) action.

Compare HSS Firmware Versions

This action compares and displays the running Halted State Services (HSS) firmware version for each Processor Blade on the system. Upon completion of the action (when state of the action is "Passed"), select the action and click **Details** to see the HSS firmware version for each Processor Blade.

Copy Core License to Alternate System Disk

Valid only for NonStop BladeSystem NB54000c and NB56000c, this action copies the core license file from \$SYSTEM to the specified alternate system disk.

Delete System Load Configuration

Allows you to delete one of the alternate system load configurations that is currently displayed under the system object attributes.

These configurations are created through the System Load Configuration action (located under the [Disk](#), [FC Disk](#), and [CLIM-Attached Disk](#) objects in the OSM Service Connection). It might be necessary to delete one of the configurations if the specified disk is no longer a valid system disk, or if you want to specify a new alternate system disk and there are already (the maximum number of) four alternate system load configurations specified.

Detect New Hardware

This action is used during service procedures to detect any new Blade Element or LSU component that had been disabled or isolated from the system by user.

NOTE: Generally, new hardware is detected dynamically once it is cabled. This action is only required for recognizing components connected on a port that had been disabled.

Enable/Disable Automation of Data Collection

Use to enable or disable automatic collection of data for failed system resources. The current state for the system is indicated by the [Automatic Data Collection State](#) attribute. If enabled, when a hardware failure occurs, data is saved to the location specified by the [Set Data Collection Volume](#) action. The [Set Days to Persist for Diagnostic Data](#) action determines how long the files are retained on the system before being deleted.

Enable/Disable Blade Power Regulator Management

This action applies to HP Integrity NonStop BladeSystem NB54000c and NB56000c only. The action enables or disables HP Power Regulator management on all processor blades in the system. Upon enabling, processor performance may immediately change in response to Power Regulator mode stored in each blade. Use HP Insight Control power management within HP SIM to view and alter the mode for each processor blade in the system.

Two attributes under the Logical attributes heading on the System object, Power Regulator Management Supported and Power Regulator Management Status, indicate whether this feature is available and enabled.

Insight Control power management is an HP SIM plug-in that can be installed after HP SIM is installed on the system console. Both HP SIM and Insight Control power management can be installed from HP Insight Control for NonStop DVD. For more information on requirements and installation instructions, see the *NonStop System Console Installer Guide*. For more information on using Insight Control power management to alter the Power Regulator mode for processor blades, see the *HP SIM for NonStop Manageability*.

Extend Problem Incident Report Suppression Time

Extends the duration of suppression by a specified amount of time (in minutes). This action fails if the suppression was not enabled at that time.

Get SMARTSSD Wear Status Summary

Launches a guided procedure that allows you to view and save a summary of the SMARTSSD wear status for any or all Solid State SAS disk drives on the system. It displays the same SMARTSSD Wear Gauge values for each drive as the [Show SMARTSSD Wear Gauge](#) action that is available on individual Solid State SAS disk drives, but this guided procedure allows you to display the information for multiple (any or all selected) drives in a single interface and to save the resulting data, if desired, in .csv (or comma delimited) format for use in Microsoft Excel.

Initialize Default Firmware File Names

Starting with H06.12, there are multiple versions of blade firmware on the SUT. The purpose of this action is to identify the proper blade firmware required for your Integrity NonStop server configuration while eliminating unnecessary firmware updates for servers that don't need the very latest blade firmware. This action, displayed only for Integrity NonStop NS14000 series and NS16000 series servers, must be performed in the following scenarios to ensure that OSM displays the proper blade firmware version information for your NonStop server:

- If you have installed a new Integrity NonStop NS16200 or NS14200 server. While new NS16200 and NS14200 systems are shipped with the proper firmware, failure to perform the action results in OSM reporting this running firmware as Up-rev. Once you perform this action, specifying NS16200 or NS14200 as your system type, OSM recognizes the running firmware as appropriate and displays the correct default firmware file names and versions.
- If you are upgrading (either completely or partially) an existing NS16000 server to NS16200 or an existing NS14000 server to NS14200, because the older blade firmware that was fine for NS16000 and NS14000 does not support the NS16200 or NS14200 (rx 2660) blades. After migrating to the appropriate RVU to support NS16200 or NS14200, the upgrade procedure directs you to perform this OSM action. Upon completion of the action, OSM displays the older running firmware as Down-rev and displays the proper default firmware file names and versions required for NS16200, NS14200, and hybrid (NS16000/NS16200 or NS14000/NS14200) systems.

If you then need to fall back to your original NS16000 or NS14000 configuration (removing all NS16200 or NS14200 processors) and want to fall back to your original firmware as well, you should perform the action again to specify NS16000 or NS14000 as the system type. OSM will then show the newer (NS16200/NS14200) firmware as Up-rev and original firmware as the appropriate minimum version to which you can fall back.

- If you are directed by the GMCSC or service provider to perform the action and choose "Recommended Fix Firmware File Set" from the list of options. This causes OSM to show the very latest blade firmware available on the SUT as the Default File Version to be used for a firmware update. This may be necessary to incorporate a recent fix not in the original minimum base firmware for your system type.

NOTE: The list of system types or configurations for which this action must be performed may grow as other hardware and/or memory configurations requiring blade software beyond the base versions required for NS16000 and NS14000 become available.

Install Core License File

Valid only for NonStop BladeSystem NB54000c and NB56000c, this action launches a guided procedure to install core license files.

NOTE: This action installs the core license files and provides an option to enable the system to run with the number of cores and processors specified in the license file. If the enable option is not selected during this procedure, the [Update Running Core License](#) action must be used for enablement.

Perform Data Sanitization

This action launches a guided procedure that provides a simple and secure method for erasing all data from disk drives that are to be retired from service. The procedure can be used to sanitize any SCSI, FC, SAS, or CLIM-attached disks that are connected to a system and are in the Down state. For more information on using the procedure, see the online help available from within the guided procedure.

Read Core License

Valid only for NonStop BladeSystem NB54000c and NB56000c, this action reads the core license file and displays (in the Action Detail dialog box) the system serial number, the number of enabled cores, and the number of enabled processors

If the core license file is missing or does not match, the action returns an error indicating that the correct license file needs to be installed.

Rediscover System

Causes OSM to refresh and reanalyze all components within the system.

Rediscover System and Cluster

Causes OSM to refresh and reanalyze all components within the system and the ServerNet cluster or NonStop BladeCluster.

NOTE: This action is not available for Integrity NonStop NS1000, NS1200, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS5000, or NS3000AC servers.

Reinitialize Complex Manager

Reinitializes the Complex Manager Auxiliary Process (CMAP) for each processor in the system. This action is intended only for Integrity NonStop NS14000 series and NS16000 series servers running H06.12 or later; it fails harmlessly (and no CMAP events are logged) when performed on other system types or when running pre-H06.12 SUTs.

⚠ CAUTION: The action should be performed only in cooperation with HP Support. If used improperly, an outage could occur. You must avoid all processor actions and cable changes while CMAP reinitialization is in progress.

It is recommended that you open an OSM event viewer session with the following retrieval criteria before proceeding with this action: \$ZLOG, using View Options - Realtime, Filter Criteria owner TANDEM, Subsys name(s) - CMAP. (To launch an event viewer session from the OSM Service Connection, it may be necessary to cancel the action, open the event viewer session, then initiate the action again.)

After clicking "Yes" to three confirmation dialog boxes and OSM reports that the action has completed successfully, check the OSM event viewer session opened earlier to locate CMAP event 135 (CMAP started reinitialization) and a corresponding CMAP event 136 (CMAP completed reinitialization) for each logical processor running NSK. Reinitialization for each processor is complete when the CMAP event 136 appears. (Other CMAP events occur as the PEs (Processor Elements) for each logical processor are rediscovered.) Once CMAP reinitialization completes successfully for all processors, you can proceed with any necessary processor actions or cable changes.

Set Data Collection Volume

Used to specify a volume in which [automatic](#) or [manual](#) data collection will take place. The volume should be something other than \$SYSTEM to avoid the possibility of filling that volume with collected data.

The [Diagnostic Data Collection Volume](#) attribute displays the currently specified volume. How long the files are retained in this volume before being automatically deleted is determined by the [Set Days to Persist for Diagnostic Data](#) action. This value is displayed by the [Days to Persist Collected Diagnostic Data](#) attribute.

Set Days to Persist for Diagnostic Data

Determines how many days the collected hardware failure data is retained on the system before being deleted. Any PAK or LOG file older than this value is deleted the next time automatic or manual data collection is initiated.

Set System Type

Specifies whether the System is a standard "Commercial" (AC-powered) or a "Central Office" (DC-powered) system.

Suppress Problem Incident Report Creation

This action, which can be initiated by a user or guided procedure, suppresses both dial-outs and the creation of Problem Incident Reports for the default time of 40 minutes. The default value can be changed in the OSMCONF file or extended for an action currently in progress by using the [Extend Problem Incident Report Suppression Time](#) action. Performing this action while the system is already in the suppressed state resets the duration of the current suppression to the default time.

Synchronize iLO Clocks to NonStop Clock

Synchronizes the iLO clock on each Processor Blade (for NonStop BladeSystems) or Blade Element (for NS-Series systems) to the NonStop system's clock. OSM does this automatically, once every 24 hours; this action allows you to synchronize the clocks immediately, as needed.

System Power Off

Puts Blade Elements, LSUs, and ServerNet enclosures into low power mode (FCDMs remain powered on).

NOTE: To power the system back on, use the [Power On System](#) action in the OSM Low-Level Link.

Test Incident Report Delivery Paths

This action tests the Incident Report delivery paths used for remote support of NonStop systems.

For HP Insight Remote Support Advanced, this action sends a periodic incident report to all incident subscribers, including every member in the fault tolerant subscriber group. OSM asks whether or not you want to delete the failed path, if one is identified by the test. An EMS event is logged containing information on connectivity from OSM to every member in the fault tolerant subscriber group. An Alarm is created if there is a problem.

For more information, see *Insight Remote Support Advanced for NonStop*, located in the Support and Service collection of NTL.

Unsuppress Problem Incident Report Creation

Removes suppression caused by the [Suppress Problem Incident Report Creation](#) action. While this suppression is automatically unsuppressed when the specified suppression time has been reached, you can choose to end the suppression immediately using this action.

Update Running Core License

Valid only for NonStop BladeSystem NB54000c and NB56000c, this action is used when a core license has been upgraded from 2-cores to 4-cores or when licenses for additional processors have been added. The action instructs system software to read the new core license file and update the core-enablement state. If the license file is valid, the action details will display the contents of the license file. If the license file is not present, an error message instructs you to perform the [Install Core License File](#) action.

Verify Power Fail Configuration

Verifies that the system is configured for Power Fail support.

Related System and Processor-Level Recovery Actions

Depending on your system type, these actions may be useful for system and processor recovery operations:

- Power On System – this OSM Low-Level Link action can be used to power on the system following power fail scenarios or after using the [System Power Off](#) action, provided you are using DNS on your LAN.
- Power Cycle All Processors – located under the Group object in the OSM Low-Level Link, this action can be used if the system is hung to power cycle all processors, processor boards, and LSUs in the system.
- For Integrity NonStop NS16000 series servers:
 - To power cycle just one processor without affecting the others, use the [Power Cycle LSU](#) action (located under the Logical Processor object in the OSM Service Connection) or use the Hard Reset action on the processor in the OSM Low-Level Link.
 - To power cycle one processor board without affecting any processors in the complex, use the [Power Down Blade Element](#) action (located under the Blade Element object in the OSM Service Connection). The Blade Element is placed in low power mode for five minutes before being powered back on.

Tape Collection

When one or more tape drives are connected to a system, a Tape Collection object appears in both the tree pane and the overview pane of the OSM Service Connection. In both panes, this object displays an alarm or yellow icon if alarms or degraded conditions exist on any of the individual tape devices contained within. You can expand the Tape Collection icon in the tree pane (but not in the overview pane) to select and monitor individual tape devices.

Location in OSM Tree: System > Tape Collection

Example: Tape Collection

Attributes

None.

Actions

None.

Tape

Specifies a tape drive configured for a system.

All tape drives are displayed under the [Tape Collection](#) object, whether they are attached through [Fibre Channel ServerNet adapters](#) in IOAM enclosures or through legacy NonStop S-series IOAM2 enclosures.

Location in OSM Tree: System > Tape Collection > Tape Drive

Slot Location:

NonStop S-Series

- Most NonStop S-series tape drives can be connected physically through a cable connected to the MFC SCSI port on the IOMF CRU or a SCSI SAC (available on a ServerNet/DA CRU or an IOMF2 CRU).
- The CT9840/CT9840FC/CT9841FC cartridge tape drives must be connected to a SCSI SAC on either a ServerNet/DA CRU or an IOMF2 CRU.

NonStop NS-Series

- Fibre Channel tape drives are connected to Fibre Channel ServerNet adapters in IOAM enclosures.
- SCSI tape drives can be connected to Fibre Channel ServerNet adapters through a [Fibre Channel Router](#) (one or two drives per router). Once configured, the Fiber Channel Router object is displayed in the OSM tree pane under the [Monitored Service LAN Devices](#) object.

Example: Tape Drive \$TAPE1

Attributes

Tape Drive

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Device State	The accessibility of the tape drive through the tape process. Values: Up, Down, Hard Down
Encryption State	Displayed only if the system is licensed for NonStop Volume Level Encryption, this attribute indicates whether or not the CLIM to which the tape drive is attached has NonStop Volume Level Encryption enabled.
Logical Device Number	The number assigned to the drive by the file system.
Product ID	The tape drive product identification.
Tape Type	The type of tape drive. Values .
Firmware Version	The version of the firmware (where applicable).
Cartridge Loader	This attribute is displayed only for certain tape drives to indicate the presence of a cartridge loader. For some newer tapes drives equipped with cartridge loaders, the attribute does not appear, but the Tape Type attribute value indicates that the drive is equipped with an ACL.

Physical

Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts. This is not the spare part number.
Serial Number	The serial number of the tape drive (where applicable).

Process Pair

Configured Processors	The two processors in which this I/O process is configured to run. Example: 0,1
Primary Execution State	The state of the primary I/O process. Values: Running, Stopped
Primary Process ID	The process ID of the primary I/O process. If the state of the primary I/O process is Stopped, this ID is not displayed. Example: 1,296
Backup Execution State	The state of the backup I/O process. Values: Running, Stopped
Backup Process ID	The process ID of the backup I/O process. If the state of the backup I/O process is Stopped, this ID is not displayed. Example: 1,285

Controller Path

Tape drives connected through an FCSA display these attributes:

FSAC	Represents the actual presence of the FCSA FSAC containing the backup tape path SCSI controller. This attribute is displayed only if the physical FCSA FSAC is present
Configured FSAC Location	Displays the configured location of the FCSA FSAC containing the backup tape path SCSI controller. This attribute is displayed even if the physical FCSA FSAC is not present.
LUN	The logical unit number of the tape. Example: 1
Port Name	A number that uniquely identifies the port through which the tape is connected.

Tape drives connected through an IOMF2 enclosure display these attributes:

SCSI ID	An identification number assigned to the device when configured.
SCSI Controller	The number (3) that identifies the SCSI controller that manages the tape drive. Example: SSAC (1.1.55.3)
Configured Controller Location	The location of the SCSI controller. Example: IOMF2.SAC-3.GRP-1.MOD-1.SLOT-55

Associated Device

Fibre Channel Router	The name of the Fibre Channel Router, as assigned through the router's web interface.
----------------------	---

CLIM Path

Configured CLIM	The CLIM to which the tape drive is configured.
HBA Location	Indicates the slot and port location for the HBA controller (either SAS or FC).
LUN	The logical unit number of the tape.

Actions

Responsive Test

Verifies that the component is installed and responding.

Start

Puts the tape process in a state to accept regular I/O commands to the tape drive. When the Start action completes, the drive is in the Started state.

Note that Start is a logical command and does not affect the hardware.

Stop

Puts the tape process in a state to disallow regular I/O commands to the tape drive. When the Stop action completes, the tape drive is in the Stopped state.

Note that Stop is a logical command and does not affect the hardware.

Switch Process Pair

Switches processors of the primary and backup tape I/O processes.

Test Extended

Tests vary depending on the type of tape drive. This table lists the actions performed for each supported tape device (listed by Product ID).

Product ID	Actions Performed
CT9840	N/A (The action can be initiated, but it will perform the same tests done by the Test Verify action.)
T514x	Data loopback test Drum motor test Servo interface loopback test
T515x	POST ROM EDC verified Queuing and enqueueing Loader software reset
T517x	N/A
T519x	Loop write-to-read. No tape (media) is required.
T9490	Microprocessor library internal loopback test Servo processor self-test Servo processor RAM test

The tape drive must be in the Stopped state to perform this action.

Test Verify

Runs the power-on self-test for the tape drive. Additionally, runs tests to isolate problems involving the tape drive, SAC, or Common Base Board. The tape drive must be in the Stopped state to perform this action.

TRSA (Token Ring ServerNet Adapter)

A customer-replaceable unit (CRU) that connects the ServerNet connections inside a server to a Token Ring LAN. The TRSA CRU contains one Token Ring ServerNet addressable controller (TRSA SAC).

Location in OSM Tree: System > Group > Module > TRSA

Slot Location: TRSA CRUs can be located in 51, 52, 53, and 54 in I/O enclosures (service side).

Example: TRSA \$ZZLAN.TRSAO (1.1.53)

Attributes

TRSA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Power State	Whether the component is powered on. Values
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the TRSA CRU and the associated Token Ring SAC. When the Abort action completes, the TRSA CRU and the Token Ring SAC are in the Stopped state.

Start

Starts the TRSA CRU and the associated Token Ring SAC. The TRSA CRU must be in the Stopped state before you perform this action.

During startup, the controller operational code is automatically loaded into the TRSA SAC. When the Start action completes, both the TRSA CRU and the Token Ring SAC are in the Started state.

Stop

Rather than automatically stopping the TRSA (as the Abort action does), this action first warns you if the TRSA is currently in use (and stops it only after you confirm).

Unknown CRU

If a service processor cannot identify a system resource, that resource is represented by an object in the tree pane. That object icon features a blue question mark.

Location in OSM Tree: System > Group > Module > Unknown CRU

Attributes

Unknown CRU

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Power State	Whether the component is powered on. Values
-------------	---

Actions

None.

UPS

Uninterruptible power supply (UPS) unit that provides backup power for Nonstop NS-series enclosures.

Location in OSM Tree: System > Monitored Service LAN Devices > UPS

Example: UPS SDUPS

Attributes

UPS

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Battery Status	Indicates the current status of the UPS battery. Possible values are Normal and On Battery. OSM displays a yellow alarm if the UPS goes On Battery (or starts drawing power from the battery). This alarm goes away when the UPS stops drawing power from the battery. OSM displays a red alarm when the battery power is low.
Device Status	Indicates whether the UPS is up or down.
Firmware Version	Version of the firmware on the UPS SNMP card.
IPv4 Address	The IPv4 address of the UPS.
Model	The model number of the UPS that was assigned in manufacturing.
Serial Number	The unique number assigned to the UPS in manufacturing. Knowing the serial number is especially helpful when you need to replace batteries or required other service. Example: TU321A1185

Software Version	Displays the version of the UPS software.
UPS Location	Displays the physical location of the UPS as set by the super-user in the Link to Web Interface action.
VA Rating	This is the apparent power rating of the UPS, expressed in Volt-Amperes. Example: 12000 VA

Physical Location

The values displayed by these attributes are assigned through the [Physical Configuration Tool](#).

Rack Name	A user-defined name assigned to identify the rack in which the UPS is located.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the UPS within the rack.

Actions

Link to Web Interface

Launches a browser-based configuration interface for the UPS, which provides additional information and configuration options for the UPS.

Rediscover

Causes OSM to refresh and reanalyze the object. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Stop Monitoring

Stops OSM from monitoring the UPS.

VIO FCSA

In a system containing VIO enclosures (represented in the OSM Service Connection as [VIO modules](#)), OSM displays an FCSA object to represent:

- In slot 1, the four built-in Fibre Channel ports that provide the functional equivalent of a Fibre Channel ServerNet adapter.
- In slot 7, an optional expansion VIO FCSA.

NOTE: VIO FCSA is not a subcomponent of VIO modules in S-series or BladeSystem NB54000c and NB56000c.

OSM does not display VIO FCSA attribute information until an associated disk process is configured and started. For more information, see the *Versatile I/O (VIO) Manual*.

Location in OSM Tree: System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > FCSA (In the Multi-Resource Actions dialog box, these FCSA objects are displayed as VIO FCSAs)

Example: FCSA (100.3.1)

Attributes

FCSA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Flash Firmware

Information about the version of the operational firmware located in the Flash memory of the FCSA.

Version	The version of the flash firmware running on the VIO FCSA.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Compare State	Indication of the differences, if any, between the current and default firmware versions. Values

Flash Boot Firmware

Information about the version of the boot firmware located in the Flash memory of the FCSA.

Version	The version of the boot firmware running on the VIO FCSA.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	Indication of the differences, if any, between the current and default firmware versions. Values

Actions

Flash Boot Firmware Update

Updates the boot firmware in Flash memory of the VIO FCSA. It is not possible to do this update unless the VIO FCSA has a disk configured through it. If the Flash Boot Firmware Compare State is Unknown, an update attempt will likely fail.

Flash Firmware Update

Updates the operational firmware in Flash memory of the VIO FCSA.

Replace

This action fails when trying to replace an FCSA in a VIO enclosure. The repair action text points you to the Support and Service collection of NTL for a documented service procedure describing how to replace a VIO FCSA.

Responsive Test

Verifies that the VIO FCSA is connected and responding.

Test Verify

Verifies basic functionality of the VIO FCSA.

VIO G4SA

In an Integrity NonStop NS-series system containing VIO enclosures (represented in the OSM Service Connection as [VIO modules](#)), OSM displays a G4SA object to represent:

- In slot 6, the Ethernet ports that provide the functional equivalent of a Gigabit 4-port Ethernet adapter.
- In slot 7, an optional expansion VIO G4SA.

In a NonStop BladeSystem NB54000c and NB56000c or NonStop S-series system containing [VIO modules](#), OSM displays a G4SA object to represent:

- In slot 6, the Ethernet ports that constitute a V4SE, which replaces a [GESA](#).
- In slot 7, for S-series only, (optional) additional ports that allow you to upgrade a V4SE to a V8SE.

Each VIO G4SA contains one [G4SA SAC](#), which contains up to four [G4SA PIFs](#), resulting in four Ethernet ports on each VIO G4SA.

Location in OSM Tree: (

- For NS-series: System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module > G4SA.
- For S-series: System > Group 11-84 > VIO Module 2 > G4SA.
- For NonStop BladeSystem NB54000c and NB56000c: System > Group 110-115 > VIO Module > G4SA.

In the Multi-Resource Actions dialog box, these G4SA objects are displayed as VIO G4SAs.

Attributes

G4SA

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Manufacturer	Identifies the manufacturer of the component. Displayed for VIO G4SAs in S-series VIO modules only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Configured Type	The configuration type of this resource. Values: CCSA, E4SA, FESA, G4SA, GESA, TRSA, Unknown
Device State	The state of the component as known to the operating system on the server. Values

Actions

Abort

Terminates operation of the VIO G4SA and the associated Ethernet ServerNet addressable controller (SAC). When the Abort action finishes, the VIO G4SA and the SAC are in the Stopped state.

Add

This action is displayed in OSM **only** when a VIO G4SA is first inserted and not yet configured. Performing this action ensures that the [Configured Type](#) is set to G4SA.

Delete

Deconfigures the VIO G4SA, removing the associated G4SA SAC and PIF objects. This action can only be performed after you delete the [LIF](#) associated with each G4SA PIF.

Power Off

Physically powers off the VIO G4SA.

Replace

Displays a service procedure describing how to replace a VIO G4SA in a VIO enclosure.

Reset

Places the VIO G4SA in a state from which it can be started.

Start

Starts the VIO G4SA and the associated G4SA SAC. The VIO G4SA and the SAC must be in the Stopped state before you perform this action.

Stop

Rather than automatically stopping the VIO G4SA (as the Abort action does), this action first warns you if the VIO G4SA is currently in use (and stops it only after you confirm).

VIO Logic Board

Component of a VIO enclosure (represented in the OSM Service Connection as a [VIO module](#)), the VIO logic board provides ServerNet connectivity between processors, ServerNet adapters, and attached hardware devices. Each VIO logic board contains five [ports](#). Ports 1 through 4 providing connectivity to processors 0 through 3. Port 5 represents the crosslink connectivity to the VIO enclosure on the opposite fabric.

OSM software communicates with an internal part of the board, represented by an IME (integrated maintenance entity) object in the OSM Low-Level Link.

Attributes

VIO Logic Board

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
LED State	Indicates whether the VIO logic board LED is on or off.
Manufacturer	Identifies the manufacturer of the component. Displayed for VIO logic board in S-series VIO modules only.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Logical

Time of Last Reset	The date and time of the last soft reset of the VIO logic board.
Fabric Side	This attribute is displayed only within the Multi-Resource Actions dialog box, to indicate whether the VIO logic board is on the X or Y fabric.

ME FPGA

Version	The VPROC of the ME FPGA (Field Programmable Gate Array) image currently loaded on the VIO logic board.
Default File Name	The full path name of the default ME FPGA file on the server.
Default File Version	The version of the ME FPGA image in the default FPGA file.
Compare State	The differences, if any, between the current and default ME FPGA versions. Values

ME Firmware

Version	The version of the ME firmware running on the VIO logic board.
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update .
Compare State	The differences, if any, between the current and default firmware versions. Values

Actions

Dump Memory

Dumps a snapshot of the VIO logic board's memory to a file in \$SYSTEM.ZSERVICE.

You can view the filename in the Action Detail dialog box for this action.

The filename convention is ZMmmmssn, where:

mmm = group number

ss = module number

n = version number (incremented for subsequent versions of the same ZMmmmss snapshot files)

Example: ZM100023: snapshot file taken of VIO logic board in group 100, module 02, version number 3.

Hard Reset

Resets the VIO logic board hardware and the routing tables.

ME FPGA Update

Allows you to update the FPGA code file for the integrated maintenance entity (IME) of the VIO logic board. The firmware file for IME FPGA (SAM0789) is different from that of other MEs.

NOTE: Because the hard reset required to complete an FPGA update disrupts a ServerNet fabric, you should perform a Check Storage Dependence on ServerNet Fabric action (on the [System](#) object) to make sure it is safe before proceeding with the FPGA update. Then update the VIO logic board on one fabric and wait at least 5 minutes after completion before checking storage dependence and updating the VIO logic board on the other fabric.

ME Firmware Update

Allows you to update the firmware file for the integrated maintenance entity (IME) of the VIO logic board. The firmware file for an IME (M1805) is different from that of other MEs.

Power Cycle

Power cycles the VIO logic board.

NOTE: This action is not valid in an S-series VIO Module.

Replace

Displays a service procedure describing how to replace a VIO logic board.

Set LED State

Turns the VIO logic board LED on or off.

Soft Reset

Reinitializes the firmware without affecting the VIO logic board hardware or the routing tables.

VIO Module

The OSM Service Connection displays a VIO Module object to represent:

- In Integrity NonStop NS14000 series, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS1200, NS1000, and NS3000AC servers, VIO enclosures, which take the place of an IOAM enclosure. There are two VIO enclosures in each system. The VIO Module objects are located under the Fabric Group objects, with VIO Module 2 under the Internal ServerNet X Fabric and VIO Module 3 under the Internal ServerNet Y Fabric.
Location in OSM Tree: System > Fabric Group 100 > Internal ServerNet Fabric > VIO Module.
For more information, see the *Versatile I/O (VIO) Manual*.
- In NonStop S-series servers, a V4SE or V8SE, which serve as a replacement for a [GESA](#). The VIO Module objects appear as modules 2 and 3 under the appropriate Group object(s).
Location in OSM Tree: System > Group 11-84 > VIO Module 2 and 3.
For more information, see the *V4SE and V8SE Enclosure Service Provider Supplement*.
- In AC-powered Integrity NonStop BladeSystems (except for NonStop BladeSystem NB50000c), two VIO Modules (Modules 2 and 3) under the appropriate Group objects (possible groups include 110-115) represent a 16-port Ethernet controller (G16SE).
Location in OSM Tree: System > Group 110-115 > VIO Module 2 and 3.

For more information, see the *G16SE Service Provider Supplement for Integrity NonStop BladeSystems*.

Each VIO Module object, depending on the type of system and configuration, contains:

- **VIO FCSA** in slot 1 – OSM displays an FCSA object to represent the four built-in Fibre Channel ports that provide the functional equivalent of an FCSA.

NOTE: Valid for NS14000 series, NS1200, and NS1000 servers only.

- (Optional) **Optical Extender PIC** in slot 2 for additional processor connectivity (processors 4-7).

NOTE: Valid for NS14000 series, NS2000 series, NS2100, NS2200 series, NS2300, NS2400 series, NS1200, and NS1000 servers only; not applicable for NS3000AC, NonStop S-series servers, or NonStop BladeSystem NB54000c and NB56000c.

- (Optional) **Optical Extender PIC** in slot 3 is valid on NS3000AC servers for NonStop S-series connectivity and on NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series servers for connecting CLuster I/O Modules (CLIMs).
- (Optional) **Optical Extender PIC** in slot 4 applies to NS2000 series, NS2100, NS2200 series, NS2300, and NS2400 series only, and is used for connecting CLuster I/O Modules (CLIMs).
- (Optional) **Optical Extender PIC** in slot 5 for ServerNet cluster connectivity.

NOTE: Valid for NS14000 servers only; not applicable for NonStop S-series, other NonStop NS-series servers, or NonStop BladeSystem NB54000c and NB56000c.

- A **VIO G4SA** in slot 6. OSM displays a G4SA object to represent the built-in Ethernet ports that provide the functional equivalent of a G4SA (NonStop BladeSystem NB54000c and NB56000c or NS-series) or GESA (S-series).
- Slot 7 can represent:
 - In NS14000 series, NS1200, and NS1000 servers, an optional expansion **VIO G4SA** or **VIO FCSA**.
 - In an S-series server, an additional VIO G4SA, which upgrades a V4SE to a V8SE (8 Gigabit Ethernet ports).
 - Not applicable for NonStop BladeSystem NB54000c and NB56000c.
- Two **VIO Power Supplies**, in slots 15 and 18.
- Two **VIO Fans**, in slots 16 and 17.
- A **VIO Logic Board** in slot 14.

VIO modules are initially configured using the **Configure Module** action in the OSM Low-Level Link, as described in the appropriate hardware installation manual for your NS-series system, the *G16SE Service Provider Supplement for Integrity NonStop BladeSystems*, or the *V4SE and V8SE Enclosure Service Provider Supplement* for S-series servers.

Attributes

VIO Module

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	A code that identifies the generation of the component. Hardware revision codes are used for tracking components.
Part Number	The part number of the component that was assigned in manufacturing. Use part numbers for identifying and ordering parts.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.

Physical Location

The values displayed by these attributes are assigned through the [Set Physical Location](#) action.

NOTE: These attributes are not displayed for a VIO Module providing V4SE or V8SE connectivity (NS16000CG or NS5000).

Rack Name	A user-defined name assigned to identify the rack in which the VIO enclosure is located. You can enter up to 15 alphanumeric characters.
Rack Offset	A number (from 1 to 42) assigned to describe the location of the VIO enclosure within the rack.
Locator	An optional text string assigned to further identify the physical location of the VIO enclosure. This attribute is displayed only if a value is specified using the Set Physical Location action.
Alarm Panel Identifier	For DC-powered Telco systems only. This attribute should not appear for VIO enclosures, as it displayed only if a value is specified through the Set Physical Location action.

Actions

Read LCD

Displays all 16 lines of the VIO enclosure's LCD text in the Action Detail dialog box.

Replace

Displays a service procedure describing how to replace a VIO enclosure.

Retrieve Network Connectivity Info

Displays remote IP addresses stored in the IPAUTH file.

NOTE: Not valid for S-series servers.

Set Physical Location

Allows you to assign these [Physical Location](#) attributes for the VIO enclosure:

- Rack Name is a user-defined name for the rack containing the VIO enclosure. You can enter up to 15 alphanumeric characters.
- Rack Offset is a numerical value representing the location of the VIO enclosure within the rack. A valid integer (from 1 to 42) must be specified when performing the Set Physical Location action, or the action will fail.
- Locator is an optional text string to help identify the physical location of the VIO enclosure. It must contain alphanumeric characters only.
- This parameter should be left blank, as it is used for DC-powered Telco systems only, which do not support VIO enclosures.

With T0682 H02 AAN and later, you can also use the [Physical Configuration Tool](#) to set the Rack Name and Rack Offset values in a consistent manner throughout the system while you create a physical view of your modular racks.

Synchronize FIR Files to Other Switches

Synchronizes the FRU information record (FIR) files of the X and Y fabric processor switches.

NOTE: This action is only valid from Group 100; it will fail on VIO Modules in NonStop BladeSystem NB54000c and NB56000c or S-series.

Write LCD Line

Allows you to edit the text displayed by the VIO enclosure's LCD. You can modify lines 9 through 15 with this action.

Common Attribute Values

Battery Charge Status

Value	Meaning
Absent	The battery is not installed.
Charged	The battery is fully charged
Charging	The battery is in the process of being charged.
Disabled	The battery cannot supply power and cannot be charged, possibly because the Disable Battery action has been performed. You should disable a battery before removal.
Discharged	The battery needs recharging or replacement.
Discharging	The system is currently drawing power from the battery.
Enabled	The battery can accept a charge and is ready to supply power if the AC power is unavailable.
Fault	Check the battery for alarms. If the condition persists, contact your service provider.
Unknown	The battery is not responding, and its state cannot be determined.

Compare State (CLIM, SAS Disk Enclosure, CLIM SAS Card, and CLIM FC Card)

Value	Meaning
Same	Current and default versions are the same.
Compatible	Available on H06.20/J06.09 and later SUTs, the current version is either newer or older than the default version, but is compatible with the default version.
Up-rev	The current version is newer than the default version. OSM version T0682 H02 ACJ (and later) supports the option of flagging Up-rev firmware on CLIM and SAS Disk Enclosure components as a problem attribute that is propagated up to parent objects in the OSM Service Connection. For information on how configure this option in your OSMCONF file, see the <i>OSM Configuration Guide</i> .
Down-rev	The current version is older than the default version.
Unknown	Unable to compare files.

Compare State (Other)

Value	Meaning
Same	Current and default versions are the same.
Up-rev	The current version is newer than the default version.
Down-rev	The current version is older than the default version.
Unknown	Unable to compare files.

Device State

Value	Meaning
Aborting	Processing is terminating.
AC Power Loss	The device is currently not powered by either AC or UPS.
Defined	State is defined by the NonStop OS.
Degraded	Performance is degraded.
Diagnose	A diagnostic test is running on the component.
Initializing	Processing is starting up.
Not Available	State is not available to OSM.
Not Configured	The component is not configured.
Not Installed	The component is not installed.
OK	Component is accessible.
On	The device is powered on.
Predictive Failure	
Started	The component is running.
Starting	Processing is starting up.
Stopped	Processing has been terminated.
Stopping	Processing is being terminated.
Unknown	Component is not responding.

Enabled State

Value	Meaning
Disabled	The component is present but not operational, possibly because the Disable action was performed.
Enabled	The component is operational.
Fault	A problem was detected. The component might be functioning below standard or not responding. Inspect the component.
Off	The component is not functional.
On	The component is functional.
Unknown	State is unknown; component might not be responding.

Group Type

A unique number in the system that identifies this group. Group Type is displayed in a window on the front door of the enclosure.

Depending on your system configuration and topology, these are the possible group numbers for processor enclosures and I/O enclosures:

Processor Enclosures	I/O Enclosures
01	11, 12, 13
02	21, 22, 23
03	31, 32, 33
04	41, 42, 43
04	51, 52, 53
06	61, 62, 63
07	71, 72, 73
08	81, 82, 83

Path State

Value	Meaning
Down	The disk path is not logically accessible. In SCF, the equivalent state is STOPPED, substate DOWN.
Exclusive Diagnostics	The processor is performing diagnostics.
Exclusive	Exclusive ownership has been declared for this disk volume, and the disk is not accessible to other users.
Format	Disk format in progress.
Hard Down	The disk volume or disk path was put in this state by an OSM Abort action or an SCF ABORT command, or it is physically inaccessible because of a hardware error. In SCF, the equivalent state is STOPPED, substate HARDDOWN.
Inaccessible	Disk cannot be accessed.
Revival	A mirrored disk is being updated.
Special Mount	Only maintenance-type I/O operations can be performed on the disk.
Unknown	The disk might not be responding.
Up	The disk path is logically accessible. This state is equivalent to the STARTED state in SCF.

Power State

Powered On	Meaning
On	Component is powered on.
Off	Component is powered off.
Possible Redundant Power Problem	There might be a problem with the backup power supply for this component. (The Redundant Power Scrub action could not determine the exact cause of the problem.)

Powered On	Meaning
Redundant Power Problem	There is a problem with the backup power supply for this component (as determined by the Redundant Power Scrub action).
Unknown	Power state of component is unknown.

Processor State

Value	Meaning
Dump in Progress	Memory is being dumped from this processor. Submit memory dumps to the your service provider for problem analysis.
Executing Diagnostics	The processor is performing diagnostics.
Frozen	The processor was frozen using the system Freeze action in the OSM Low-Level Link application.
Frozen by Other Processor	This freeze-enabled processor froze when another processor asserted system freeze.
Halted	The processor is halted.
Hardware Error Freeze	The processor has asserted system freeze.
Hung	The processor has stopped responding
Offline Diagnostics Running	Component is unavailable due to offline diagnostic testing.
Primed For Dump	The processor is primed for memory dump. Submit memory dumps to your service provider for problem analysis.
Primed For Reload	The processor is primed for system load.
Primed For ServerNet Dump	The processor is primed for a memory dump using ServerNet. Submit memory dumps to your service provider for problem analysis.
Primed for ServerNet Load	The processor is primed for system load using ServerNet.
Processor Hung	The processor has stopped responding.
Reload In Progress	The system is reloading.
Running NSK	The processor is executing the operating system.
ServerNet Dump in Progress	This processor is dumping memory over ServerNet. Submit memory dumps to your service provider for problem analysis.
ServerNet Load In Progress	The system is loading over ServerNet
Undefined	The state of the processor cannot be determined.
Unknown	The processor is not responding.

Processor Type

Type	System
NSR-W	S7000
NSR-D	S7400
NSR-E	S7600
NSR-J	S7800
NSR-S	S7800B

Type	System
NSR-G	S70000
NSR-T	S72000
NSR-V	S74000
NSR-X	S76000
NSR-H	S78000
NSR-Y	S86000
NSR-Z	S88000
NSE-A	Integrity NonStop NS16000 server
NSE-AB	Integrity NonStop BladeSystem NB54000
NSE-AD	Integrity NonStop NS2200 series server
NSE-AE	Integrity NonStop NS2100 server
NSE-AF	Integrity NonStop BladeSystem NB56000
NSE-AG	Integrity NonStop NS2300 server
NSE-AH	Integrity NonStop NS2400 series server
NSE-B	Integrity NonStop NS1000 server
NSE-D	Integrity NonStop NS14000 server
NSE-I	Integrity NonStop NonStop NS5000T or NS5000CG server
NSE-K	Integrity NonStop NS3000AC server
NSE-M	Integrity NonStop BladeSystem NB50000
NSE-Q	Integrity NonStop NS1200 server
NSE-S	Integrity NonStop NS14200 server
NSE-T	Integrity NonStop NS16200 server
NSE-W	Integrity NonStop NS2000 series server

Service State

Value	Meaning
OK	The object is functioning properly. This value appears only in the Problem Summary dialog box.
Attention Required	The resource requires operator attention. This condition sometimes generates an alarm, and the component that requires attention is colored yellow in the tree pane and in the Physical and ServerNet views of the view pane.
Service Required	The resource requires service. This condition generates an alarm, and the component that requires service is colored red in the tree pane and in the Physical and ServerNet views of the view pane.
Problem Acknowledged	The alarm that caused the Service State to display degraded values has been suppressed. (Degraded Service State values are caused by alarms. While you cannot suppress the Service State attribute, you can suppress the alarm that causes the degraded attribute value.)

Tape Types

Product ID	Meaning
CT9840-1	9840 cartridge tape drive mounted in an L700 tape library
CT9840-2	9840 cartridge tape drive mounted in a 9710 tape library
CT9840-3	9840 cartridge tape drive mounted on HP NonStop S-series server
CT9840-4	9840 cartridge tape drive mounted in a 9310 tape library
CT9840FC-1	9840FC (Fibre Channel) cartridge tape drive mounted in an L700 tape library
CT9840FC-3	9840FC (Fibre Channel) cartridge tape drive mounted on HP NonStop S-series server
CT9840FC-4	9840FC (Fibre Channel) cartridge tape drive mounted in a 9310 tape library
CT9841FC-1	Fibre Channel 9841 cartridge tape drive mounted in an L700 tape library
CT9841FC-4	Fibre Channel 9841 cartridge tape drive mounted in a 9310 tape library
EZX-A0	EZX Controller model A0/ETI-NET, Inc
M8501	HP Ultrium 960 LTO Fibre Channel Tape Drive w/ACL - rack mount
M8502	HP Ultrium 960 LTO Fibre Channel Tape Drive w/ACL - table top
M8503	HP Ultrium 960 LTO Fibre Channel Tape Drive in L700 tape library
M8504	HP Ultrium 960 LTO Fibre Channel Tape Drive in mid-range tape library
M8505	HP Ultrium 960 LTO Fibre Channel Tape Drive - table top
N1521A	HP Ultrium 460 LTO Fibre Channel Tape Drive in L700 tape library
N1522A	LTO in mid-range tape library
N1524A	LTO with ACL installed in tape enclosure
N1525A	LTO with ACL - table top model
N1526A	HP Ultrium 460 LTO Fibre Channel Tape Drive - rack mount
N1527A	HP Ultrium 460 LTO Fibre Channel Tape Drive - table top
T5142	Digital audio tape (DAT) recording device
T5142ACL	Digital audio tape (DAT) recording device with ACL
T515 (7-9)	Digital linear tape (DLT 4000 or 7000) subsystem
T517x	Open reel tape
T519x	18 or 36-track tape cartridge subsystem
T5242	Tabletop, manual-load DAT 72 recording device
T5242ACL	Tabletop DAT 72 recording device with ACL
T5242-2SE	Rack-mounted, dual-drive DAT 72 recording device for Central Office servers
T5243	HP DAT 72 - table top, manual load
T5243ACL	HP DAT 72 - table top, with ACL
T5243-2SE	HP DAT 72 - two drive unit
T5257	Super DLT installed in HP NonStop S-series tape enclosure
T5257ACL	Super DLT with ACL installed in HP NonStop S-series tape enclosure
T5259	Super DLT for mounting in the CTL700 or CTL700/M automated tape library

Product ID	Meaning
T5258ACL	Super DLT tabletop with ACL
T9490	STK 9490 cartridge drive
VT5801	Virtual Tape Solution: Tributary Systems Inc. 2U
VT5802	Virtual Tape Solution: Tributary Systems Inc. 7U
VT5900-A	Virtual Tape Solution: Tape Labs Inc. 7U
VT5900-B	Virtual Tape Solution: Tape Labs Inc. 7U
VT5900-C	Virtual Tape Solution: Tape Labs Inc. 7U
VT5901	Virtual Tape Solution: Tape Labs Inc. 2U
VT5902	Virtual Tape Solution: Tape Labs Inc. 7U

Topology

Value	Meaning
Error	Not all service processors are set to the same value of either 8 or 16.
Retrieving	System is retrieving topology information.
Tetra 8	The system configuration is set to support a maximum of 8 processors.
Tetra 16	The system configuration is set to support a maximum of 16 processors.
Unknown	Topology information cannot be determined.

12 Managing a ServerNet Cluster

A ServerNet cluster is a collection of NonStop servers connected together using the ServerNet protocol. There are two generations of ServerNet clusters that utilize cluster switches for ServerNet cluster connectivity:

- The first-generation ServerNet cluster is built around the HP NonStop Cluster Switch (model 6770) and can support up to 24 nodes. It is built using one of the star topologies (star, split-star, or tri-star).

For information about ServerNet clusters built with the star topologies, see the *ServerNet Cluster Manual*, the *ServerNet Cluster 6770 Hardware Installation and Support Guide*, and the *ServerNet Cluster Supplement for NS-Series Servers*.

- The second-generation ServerNet cluster is built around the HP NonStop ServerNet Switch (model 6780) and can support up to 64 nodes. It is built using a layered topology.

For information about ServerNet clusters built with the layered topology, see the *ServerNet Cluster 6780 Planning and Installation Guide*, the *ServerNet Cluster 6780 Operations Guide*, and the *ServerNet Cluster Supplement for NS-Series Servers*.

HP NonStop [BladeCluster Solution](#) offers a topology, for NonStop BladeSystems and NS16000 series servers only, that requires no additional cluster switches for ServerNet cluster connectivity.

Using the OSM Service Connection, you can monitor and maintain the ServerNet cluster resources. The hardware resources in a cluster differ depending on the topology of the ServerNet cluster. For details about the resources that make up each type of ServerNet cluster, see [Cluster Resources](#).

BladeCluster Solution

A clustering topology for HP Integrity NonStop BladeSystems and Integrity NonStop NS16000 series servers only that provides connectivity directly through the ServerNet switches in the Blade enclosure or P-switches, without the need for additional cluster switches.

To configure a system as a member of a BladeCluster, use the [Add Node to ServerNet Cluster](#) action, located under the System object. Once configured through the guided procedure, the OSM Service Connection displays a [BladeCluster](#) object in the tree pane (instead of a ServerNet Cluster object, as with other ServerNet Cluster topologies), at the same level as the System object. Under the BladeCluster object, OSM displays a [Node](#) object for every member of the BladeCluster. The system to which the OSM session is logged on is represented by a Local Node object; all other member systems are represented by a Remote Node object.

For H06.23/J06.12 and later, BladeCluster enhancements include support for additional long distance options of 50 kilometers and 65 kilometers maximum between zones in a BladeCluster topology. For more information, see the *BladeCluster Solution Manual*.

Locating and Viewing Cluster Resources

To locate resources in a ServerNet cluster, expand the ServerNet Cluster resource in the tree pane to see the resources and connections in the cluster.

To view more information about a particular resource:

1. In the tree pane, select the resource.
2. In the details pane:
 - Click the Attributes tab to see attributes for the resource.
 - Click the Alarms tab to see if there are alarms for the resource.

In the View drop-down list, you can select different views of the ServerNet cluster:

- The Physical view depicts the connections and resources within the ServerNet cluster.
- The Inventory view lists the ServerNet cluster resources in tabular format.

See also [Using the Browser's Find Feature](#).

Monitoring a Cluster

ServerNet cluster monitoring tasks include:

- Viewing alarms for resources in a ServerNet cluster.
This task is similar to viewing alarms for resources within a server, except that you must first select the ServerNet Cluster in the tree pane and then navigate to the cluster resource you want to view. See [Viewing a Summary of Alarms](#).
- Viewing attributes for resources in a ServerNet cluster.
This task is similar to viewing attributes for resources within a server. See [Viewing Attributes](#).
- Checking for Incident Reports. OSM generates problem incident reports when critical changes occur to a resource and sends them to Insight Remote Support Advanced.
- Checking the OSM Event Viewer for events.
The [OSM Event Viewer](#) displays events from EMS-formatted log files such as \$0 and \$ZLOG.
- Checking the status of the ServerNet cluster subsystem (\$ZZSCL).
Navigate to the ServerNet Cluster resource and check the value of the ServerNet Cluster State attribute.
- Monitoring the Expand-over-ServerNet lines.
Navigate to a Remote ServerNet Node resource and check the value of the Line LDEV State attribute. This value indicates the state of the line between the local node and the selected remote node. Repeat this action for all remote nodes in the cluster.

Performing Actions on Cluster Resources

Some of the actions you can perform on resources within a ServerNet cluster include:

- Testing ServerNet cluster connectivity. Perform the [Node Connectivity ServerNet Path Test](#) for the external ServerNet fabrics, the [Node Responsive Test](#) for the 6780 switch node port, and the [Responsive Test](#) for the 6780 switch module.
- Starting and stopping the ServerNet cluster subsystem (\$ZZSCL). Perform the [Set ServerNet Cluster State](#) action on the ServerNet Cluster resource.
- Switching the primary and backup processors for SANMAN and SNETMON. Perform the [Switch SANMAN Process Pair](#) and [Switch SNETMON Process Pair](#) actions on the ServerNet Cluster resource.
- Setting LEDs on switch or switch components to blink so the resource can be easily located. Perform the Blink LED action for 6780 switch components and the Blink All LEDs action for the 6780 switch module. For the ServerNet II switch component of the 6770 switch, perform the Blink LED action.
- Assigning a text string to help locate a cluster switch. See [Specifying a Cluster Switch Locator String](#).
- Updating firmware, configuration, and FPGA code for the 6780 ServerNet switch. Perform the [Firmware Update](#), [Configuration Update](#), and [FPGA Update](#) actions on the switch logic board component.

- Updating firmware and configuration for the 6770 cluster switch. Perform the [Firmware Update](#) and [Configuration Update](#) actions on the ServerNet II switch component.
- Replacing components of a cluster switch using the Replace Switch guided procedure. To launch the guided procedure, navigate to the switch component and perform the Replace action.

Performing actions on ServerNet cluster resources is similar to [performing actions on resources](#) within a server. First expand the ServerNet Cluster resource in the tree pane and then navigate to the cluster resource on which you want to perform an action.

Specifying a Cluster Switch Locator String

The Set Locator action allows you to specify a text string to indicate the physical location of a cluster switch. This information, which appears in the Locator attribute for the cluster switch, assists in locating the switch when maintenance is required.

The maximum length for the text string (including spaces) is:

- 64 characters for the 6780 switch
- 32 characters for the 6770 switch

To specify the switch location:

1. In the tree pane, expand the ServerNet Cluster.
2. Expand the external fabric on which the switch is located.
3. Navigate to the switch module and right-click it.
4. From the menu, select **Actions**.
5. From the Available Actions, select **Set Locator**.
6. Click **Perform Action**.
7. In the Locator box, type descriptive text to indicate where the switch is located (for example, BLDG 12, ROOM 2154, SOUTH WALL).
8. Click **OK**. Monitor the Action Status box for a message indicating completion of the action.
9. Close the Actions dialog box.

The switch location text appears in the Locator attribute for the cluster switch.

Updating Cluster Switches

To update the firmware, configuration, and FPGA images for the switch logic board in a 6780 switch module, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

Use these procedures to update firmware and configuration on the ServerNet II Switch component of a 6770 switch module. When performing these updates:

- Update firmware before updating the configuration.
- Do not perform concurrent Firmware Update actions on the same ServerNet II switch.

Updating ServerNet II Switch Firmware

To update ServerNet II switch firmware:

1. In the tree pane of the OSM management window, expand the ServerNet Cluster resource and navigate to the switch component of the switch module.
2. Right-click the Switch component and select **Attributes**. In the Firmware section, check the value of the Compare State attribute. If it is Down-rev, continue with this procedure.
3. Right-click the Switch component and select **Actions**. The Actions dialog box appears.
4. In the Available Actions drop-down list, select the **Firmware Update** action and then click **Perform action**. Follow the screen prompts and monitor the status of the action.
5. When the update is complete, right-click the Switch component and then select **Attributes**. In the Firmware section, confirm that the value of the Compare State attribute is Same.

Updating ServerNet II Switch Configuration

NOTE: You can change the configuration tag as part of the Update Configuration action. However, you normally do this only when you are changing to a different network topology for a ServerNet cluster. See [Updating ServerNet Cluster Topology](#).

To update ServerNet II Switch configuration:

1. In the tree pane of the OSM management window, expand the ServerNet Cluster resource and navigate to the Switch component of the Switch Module.
2. Right-click the Switch component and select **Attributes**. In the Configuration section, check the value of the Compare State attribute. If it is Down-rev, continue with this procedure.
3. Right-click the Switch component and select **Actions**. The Actions dialog box appears.
4. In the Available Actions drop-down list, select the **Configuration Update** action and click **Perform action**. Follow the screen prompts and monitor the status of the action.
5. When you are prompted to perform a Hard Reset action:
 - Click **Yes** to perform the reset now. ServerNet traffic through the switch is temporarily disrupted.
 - Click **No** if you want to wait until later. The new configuration does not take effect until you perform the Hard Reset action.
6. When the reset is complete, right-click the Switch component and select **Attributes**. In the Configuration section, confirm that the value of the Compare State attribute is Same.

Managing One of the Star Topologies With OSM

OSM supports all topologies of a ServerNet cluster: the star topologies (star, split-star, and tri-star) and the newer layered topology.

Router Connections in a Layered Topology

Router Connections for Switch Node Ports

External Slot	Port	Internal Router	Port
6	1	1	0
	2	1	1
7	1	2	0
	2	2	1
8	1	3	0
	2	3	1
9	1	4	0
	2	4	1

Router Connections for Ports Connecting to Other Switches

	External Slot	Port	Internal Router	Port
Zone	2	1	5	6
		2	5	7
	3	1	5	8

	External Slot	Port	Internal Router	Port
		2	5	5
Layer	11	1	3	7
		2	4	7
		3	1	7
		4	2	7
	12	1	2	8
		2	1	8
		3	4	8
		4	3	8
	13	1	1	9
		2	2	9
		3	3	9
		4	4	9

Router Connections for Router Interconnect PICs

External Slot	Internal Router	Port
Slot 4	1	4
	2	5
	3	4
	3	5
Slot 5	1	6
	2	4
	3	5
	4	4

13 Cluster Resources

A ServerNet cluster is built using one of several topologies. The resource objects displayed in the OSM Service Connection for a cluster differ depending on the topology of the ServerNet cluster.

ServerNet clusters using one of the star topologies are built with the HP NonStop Cluster Switch (model 6770) and can support up to 24 nodes.

ServerNet clusters using the layered topology are built around the HP NonStop ServerNet Switch (model 6780) and can support up to 64 nodes.

Resource Objects in the Star Topologies	Resource Objects in the Layered Topology
ServerNet Cluster	ServerNet Cluster
External ServerNet Fabric	External ServerNet Fabric
	Switch Group
6770 Switch Module <ul style="list-style-type: none">• ServerNet II Switch• Switch-to-Node PIC• Switch-to-Switch PIC• AC Transfer Switch• UPS (6770 Switch Module)	6780 Switch Module <ul style="list-style-type: none">• Switch Logic Board• Switch PIC• Switch Port• Switch Node Port• Switch Power Supply• Switch Fan
Remote 6770 Switch	
ServerNet Local Node	ServerNet Local Node
ServerNet Remote Node	ServerNet Remote Node

Resource Objects in the BladeCluster Topology

For NonStop BladeSystems and NS 16000 series servers only, the [BladeCluster Solution](#) topology provides a clustering topology that permits connectivity directly through the ServerNet switches in the Blade enclosure or P-switches, without need for additional cluster switches. The objects displayed in the OSM Service Connection when the system is a member of a BladeCluster include:

- [BladeCluster](#)
- [Local Node](#)
- [Remote Node](#)

6770 Switch Module

A hardware assembly that provides connectivity for multiple nodes of a ServerNet cluster. The 6770 switch module is used in star, split-star, and tri-star topologies. The subcomponents of the 6770 switch module are the [ServerNet II Switch](#), the [AC Transfer Switch](#), and the [Uninterruptible Power Supply \(UPS\)](#).

Location in OSM tree: Under the External ServerNet Fabric (X and Y) objects.

Example: SwitchModule \$ZZSMN.Y1

Attributes

Switch Module

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Presence	Whether the switch is installed and responding. Values: Present, Absent, and Unknown
Locator	User-assigned text that can be used to help identify the switch. The text is assigned by using the Set Locator action. Example: Switch On Left in 1205
Topology	The network topology and ServerNet nodes supported by this 6770 switch. The value is equivalent to the configuration tag of the ServerNet II switch. Values

Actions

Replace

Launches an interactive procedure that provides help for replacing switch components.

Set Locator

This action allows you to enter text to aid in locating or identifying the switch. This text appears as the Locator attribute. These ASCII characters cannot be used in the Set Locator field: =, +, &, or %. Also, copy and paste features do not work in this field. For more information, see [Specifying a Cluster Switch Locator String](#).

Value: Free-form text up to 64 characters long.

Example: Switch On Left in 1205

SCF Equivalent: SCF ALTER SWITCH \$ZZSMN, NEAREST { X | Y}, LOCATOR string

6780 Switch Module

A hardware component that provides connectivity for multiple nodes of a second-generation ServerNet cluster using the layered topology. As part of the layered topology, the 6780 switch module comprises one cluster switch layer within a cluster switch group. The 6780 switch connects to the nodes through fiber-optic cables.

The subcomponents of the 6780 switch module are the [Switch Logic Board](#), [Switch PICs](#), [Switch Ports](#), [Switch Power Supply](#), and [Switch Fan](#).

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module

Example: witch Module \$ZZSMN.Y21 (1021.1)

[The 6780 switch module on the Y fabric of zone 2, occupying layer 1]

Attributes

Switch Module

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Midplane Physical

Primary AC Power State	Whether the primary power source is On or Off.
Backup AC Power State	Whether the backup power source is On or Off.
Part Number	The part number of the switch module midplane.
Presence	Whether the switch module is installed and responding. Values: Present, Absent, and Unknown
Track ID	The track ID of the switch module midplane.
Manufacturer	Identifies the manufacturer of the component.
Hardware Revision	The hardware revision of the switch module midplane.

Logical

Globally Unique ID	A unique, read-only number stored in nonvolatile memory (EEPROM) on a cluster switch. The Globally Unique ID can be used programmatically to identify the switch.
Current Numeric Selector Setting	The current value of the 4-digit numeric selector setting. Example: 9621
Locator	User-assigned text, that can be used to help identify the module. The text is assigned by using the Set Locator action. Example: Switch Group On Right in 1206
Numeric Selector Setting Used by Firmware	The 4-digit numeric selector setting that is currently used by the firmware. Example: 9621

Temperature

Current Value	The current temperature, in degrees Celsius (°C), inside the enclosure of the module.
Normal Maximum Value	The maximum acceptable air intake temperature is 65 degrees Celsius. If the temperature rises above 65 degrees, an alarm is generated.

Actions

Blink All LEDs Off

Turns off the blinking of the fault LEDs on the switch logic board, PICs, power supplies and fans.

SCF Equivalent: ALTER SWITCH, BLINK NONE

Blink All LEDs On

Causes the fault LEDs on the switch logic board, PICs, power supplies, and fans to start blinking.

SCF Equivalent: ALTER SWITCH, BLINK ALL

Connect to UPS

Starts a new Internet Explorer window and loads the default HTTP home page provided by the UPS vendor.

Parameter: IP Address (the IP address of the UPS)

Replace

Invokes the Replace Switch Component guided procedure that helps to replace the switch module.

Responsive Test

Tests the connectivity of the switch module from the local node.

Set Locator

Allows you to enter text to aid in locating or identifying the switch. This text is displayed as the Locator attribute. These ASCII characters cannot be used in the Set Locator field: =, +, &, or %. Also, copy and paste features do not work in this field. For more information, see [Specifying a Cluster Switch Locator String](#).

Parameter: Locator – Free-form text up to 64 characters long.

Example: Switch On Left in 1205

SCF Equivalent: SCF ALTER SWITCH \$ZZSMN, FABRIC { X | Y }, ZONE { 1 | 2 | 3 }, LAYER { 1 | 2 | 3 | 4 }, LOCATOR string

AC Transfer Switch

A component of a 6770 switch module that automatically switches to a backup AC power source if the primary source fails.

Location in OSM tree: External ServerNet Fabric > Switch Module > AC Transfer Switch

Example: AC Transfer Switch \$ZSMN.X1

Attributes

AC Transfer Switch

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Backup Rail Power State	The state (On or Off) of the backup power source for the switch. If both the primary and backup sources of power fail, the UPS provides two hours of backup power.
Primary Rail Power State	The state (On or Off) of the primary power source for the switch. If both the primary and backup sources of power fail, the UPS provides two hours of backup power.

Actions

Replace

Launches the Replace Switch Component guided procedure, which provides help for replacing the component.

BladeCluster

The BladeCluster object is displayed at the top level of the tree pane when a NonStop BladeSystem or NS16000 series server is a member of a [BladeCluster](#). A system is added to a BladeCluster using the [Add Node to ServerNet Cluster](#) action.

The BladeCluster object can be expanded in the tree pane to see [Node](#) objects representing the local and all remote nodes in the BladeCluster zone.

Location in OSM tree: Located at the top level.

Attributes

BladeCluster

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

BladeCluster Service

ServerNet Cluster State	The current state of the ServerNet Cluster subsystem on the local node. Values: Starting, Started, Stopping, Stopped, and Unknown SCF Equivalent: SCF STATUS SUBSYS \$ZZSCL
-------------------------	---

Logical

Inter-Zone Distance	Indicates whether the distance is Short-Haul or Long-Haul.
Local Node Position	The node position of this system as a member node of a BladeCluster; possible values being 1-8.
Local Zone Number	The zone number of this system as a member node of a BladeCluster; possible values being 1, 2, or 3.
Node in Service	When the Place Local Node in Service action has been performed, this attribute displays with a value of Yes, indicating that alarms will not be dialed out on this remote node from other directly-connected nodes. This particular state of alarm suppression ends when OSM CIMOM is restarted; at which time this attribute would display a value of No, and any subsequent system halt or stopping of SNETMON would once again trigger alarms on the other directly-connected nodes.
Number of Zones	Displays the configured number of zones for this BladeCluster. For the current release, only one zone is supported.
SNETMON Version	Displays the VPROC of SNETMON for the current SYSnn.

Actions

Place Local Node in Service

This action can be used before intentionally halting a system or stopping SNETMON to prevent all other directly-connected nodes from dialing out an alarm as soon as SNETMON is stopped or the node is halted. Upon performing the action, the Node in Service attribute displays a value of Yes.

This particular state of alarm suppression ends when OSM CIMOM is restarted; at which time the Node in Service attribute returns to displaying a value of No, indicating that any subsequent system halt or stopping of SNETMON would trigger alarms on the other directly-connected nodes.

Reset ServerNet Statistics

Resets the ServerNet statistical counters to zero for all processors in the system. You can use this action before performing a specific system activity and then use the Generate ServerNet Statistics action to get statistics on that system activity.

ServerNet Path Test on X Fabric

Runs a path test on the X fabric, checking the local node's connection to the BladeCluster by testing the X fabric between the local node and remote nodes.

ServerNet Path Test on Y Fabric

Runs a path test on the Y fabric, checking the local node's connection to the BladeCluster by testing the Y fabric between the local node and remote nodes.

Set ServerNet Cluster State

Starts or stops the ServerNet Cluster subsystem on the local node.

Parameter: ServerNet Cluster State can be set to Stopped or Started.

External ServerNet Fabric

This object represents a collection of switches and ServerNet links that connect the local node to other nodes in a ServerNet cluster.

Location in OSM tree:The External ServerNet Fabrics (X and Y) are under the ServerNet Cluster.

Example:External ServerNet X Fabric

Attributes

External ServerNet X Fabric

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Number of Nodes	The number of nodes that are currently connected to the ServerNet cluster on this fabric, including the local node to which you are currently logged on.
Fabric State	<p>The connectivity state between processors on the local node and processors on remote nodes for this fabric.</p> <p>Up: At least one processor on the local node can communicate with a processor on one of the remote nodes.</p> <p>Down: No processor on the local node can communicate with a processor on any remote node. This value is the default.</p>

Actions

Node Connectivity ServerNet Path Test

Checks the local node's connection to the ServerNet cluster by testing the external fabric (X or Y) between the local node and the cluster switch on the fabric. For NS16000 series servers, connection to the local node is made through cluster PICs (slot 2) on the processor switches. For NS14000 servers, the connection to the local node is made through a ports on the ServerNet Switch Boards in the IOAM enclosure.

Local or Remote BladeCluster Node

When a NonStop BladeSystem or NS16000 series server is a member of a BladeCluster, OSM displays node objects representing each member of the cluster beneath the [BladeCluster](#) object in the tree pane. The Local Node object represents the system that the OSM session is logged on to; Remote Node objects represents all other nodes in the BladeCluster.

Location in OSM tree: Located at the top level.

Attributes

Logical

Expand Node Number	The Expand node number of the local node. Value: 0 through 254
Node Name	The Expand name of the local node.
Node Position in the Zone	The position of the local node in the zone.
ServerNet Node Number	The ServerNet node number of the local node.
X Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet X fabric. Up: At least one of the processors on the local node can communicate with at least one processor on a remote node over the X fabric. Down: No processor on the local node can communicate with any processor on the remote node over the X fabric. Partially Connected. Unknown: The state of the connection cannot be determined.
Y Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet Y fabric. Up: At least one of the processors on the local node can communicate with at least one processor on a remote node over the Y fabric. Down: No processor on the local node can communicate with any processor on the remote node over the Y fabric. Partially Connected. Unknown: The state of the connection cannot be determined.
Zone Number	The number of the local node's zone in the BladeCluster. For the current release, only one zone is supported.

Expand_Over_ServerNet Configuration

These attributes are displayed only for the Remote Nodes.

Connectivity State	The state of the Expand-over-ServerNet connection from the local node to the remote node. Values: Connected, Not Connected
Line LDEV Name	The name assigned to the Expand-over-ServerNet line configured from the local node to the selected remote node. Example: \$SC212
Line LDEV	The logical device (LDEV) number of the Expand-over-ServerNet line configured from the local node to the selected remote node. Example: 121
Line LDEV State	The state of the Expand-over-ServerNet line configured from the local node to the selected remote node. Values: Up, Down, Not Available
Remote Line LDEV State	The state of the Expand-over-ServerNet line configured from the remote node to the local node. Values: Up, Down, Unknown

Y Fabric Connection #1

Port Name	Identifies the Y1 port used for BladeCluster connectivity.
-----------	--

Y Fabric Connection #2

Port Name	Identifies the Y2 port used for BladeCluster connectivity.
-----------	--

X Fabric Connection #1

Port Name	Identifies the X1 port used for BladeCluster connectivity.
-----------	--

X Fabric Connection #2

Port Name	Identifies the X2 port used for BladeCluster connectivity.
-----------	--

Actions

Generate ServerNet Statistics

Generates an event containing the ServerNet statistics for the node.

X Fabric Responsive Test

Issues a responsive test to test the connectivity between this node and other nodes on the X fabric.

Y Fabric Responsive Test

Issues a responsive test to test the connectivity between this node and other nodes on the Y fabric.

Remote 6770 Switch

The nodes connected directly to one switch see the other switches as remote switches. Although local and remote switches are the same from a hardware standpoint, less information and no actions are available for the remote switch. To perform actions or get additional information on a remote switch, establish a service connection from one of the nodes that connects directly to that switch.

Location in OSM tree: External ServerNet Fabric > Remote Switch

The last part of the switch name indicates the fabric and position of the switch in the topology.

Example: Remote Switch \$ZZSMN.X2

Attributes

Remote Switch

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Configuration Tag	A parameter used by SCF and the guided procedures that allows SANMAN to select an appropriate switch configuration block (SCB) from the M6770CL switch configuration library. The selected SCB is subsequently loaded on the specified switch. The configuration tag determines the position of the cluster switch in the topology and the ServerNet node numbers supported by the cluster switch. Values Example: Max 24 nodes, nodes 1-8
GUID	A unique, read-only number stored in nonvolatile memory (EEPROM) on a ServerNet II switch. The Globally Unique ID can be used programmatically to identify the switch.

Fabric Setting	Whether the switch is configured for operation on the X fabric or the Y fabric. Values: X, Y, or Clear
Presence	Verification that the switch is installed and responding. Values: Present, Absent, Unknown
Configuration Version	The version of the configuration file currently loaded on the switch. Example: 1_5
Firmware Version	The version of the firmware currently loaded on the switch. Example: 3_0_23

Actions

None.

ServerNet Cluster

A ServerNet cluster is a collection of NonStop servers connected together that function as a single processing unit. Servers within a ServerNet cluster pass information to each other using the ServerNet protocol.

Location in OSM tree: Located at the top level.

See also [Managing a ServerNet Cluster](#).

Attributes

ServerNet Cluster

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

SNETMON Version	The software version of the SNETMON process (\$ZZSCL). Example: SCL - T0294G08 - (11AUG03) - (07JUL03) - (AAL)
Maximum Number of Nodes	The number of ServerNet nodes that are possible with the current topology of the cluster.
Current Number of Nodes	The number of ServerNet nodes that are currently members of this cluster.

ServerNet Cluster Service

ServerNet Cluster State	The current state of the ServerNet Cluster subsystem on the local node. Values: Starting, Started, Stopping, Stopped, and Unknown SCF Equivalent: SCF STATUS SUBSYS \$ZZSCL
-------------------------	---

SANMAN Process Pair

Primary Execution State	The state of the primary SANMAN process. Values: Running, Stopped
Primary Process ID	The process ID of the primary SANMAN process. If the state of the primary SANMAN process is Stopped, this ID is not displayed. Example: 1,296

Backup Execution State	The state of the backup SANMAN process. Values: Running, Stopped
Backup Process ID	The process ID of the backup SANMAN process. If the state of the backup SANMAN process is Stopped, this ID is not displayed. Example: 1,285

SNETMON Process Pair

Primary Execution State	The state of the primary SNETMON process. Values: Running, Stopped
Primary Process ID	The process ID of the primary SNETMON process. If the state of the primary SNETMON process is Stopped, this ID is not displayed. Example: 1,296
Backup Execution State	The state of the backup SNETMON process. Values: Running, Stopped
Backup Process ID	The process ID of the backup SNETMON process. If the state of the backup SNETMON process is Stopped, this ID is not displayed. Example: 1,285

Actions

Rediscover

Causes OSM to refresh and reanalyze the object and all subcomponents. Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

Reset ServerNet Statistics

Resets the ServerNet statistical counters to zero for all processors in the system. You can use this action before performing a specific system activity and then use the Generate ServerNet Statistics action to get statistics on that system activity.

SCF Equivalent: SCF START SUBSYS \$ZZSCL

Set ServerNet Cluster State

Starts or stops the ServerNet Cluster subsystem on the local node.

Parameter: ServerNet Cluster State can be set to Stopped or Started.

Switch SANMAN Process Pair

Switches the SANMAN process from the primary processor to the backup processor.

SCF Equivalent: SCF PRIMARY \$ZZSMN

Switch SNETMON Process Pair

Switches the SNETMON process from the primary processor to the backup processor.

SCF Equivalent: SCF PRIMARY \$ZZSCL

Update Topology

Launches an interactive action that guides you in updating the network topology of a ServerNet cluster. You are prompted to temporarily disable dial-out alarms during the update process. For more information, see [Updating ServerNet Cluster Topology](#).

ServerNet Local Node

This object represents the system within a ServerNet cluster to which you are currently logged on.

Location in OSM tree: Under the ServerNet Cluster

Example: ServerNet Local Node \STARZ

Attributes

ServerNet Local Node

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Y Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet Y fabric. Up: At least one of the processors on the local node can communicate with at least one processor on a remote node over the Y fabric. Down: No processor on the local node can communicate with any processor on the remote node over the Y fabric. Unknown: The state of the connection cannot be determined.
Expand Node Number	The Expand node number of the local node. Value: 0 through 254
ServerNet Node Number	The ServerNet node number of the local node. Value: 1 through 96
X Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet X fabric. Up: At least one of the processors on the local node can communicate with at least one processor on a remote node over the X fabric. Down: No processor on the local node can communicate with any processor on the remote node over the X fabric. Unknown: The state of the connection cannot be determined.

Actions

Generate ServerNet Statistics

Generates an event containing the ServerNet statistics from the remote node to the local node.

ServerNet Remote Node

This object represents any system within a ServerNet cluster that is not the local node. Remote nodes are visible when the ServerNet Cluster view is selected.

Location in OSM tree: Under the ServerNet Cluster

Example: ServerNet Remote Node \MOON2

Attributes

ServerNet Remote Node

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Y Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet Y fabric. Up: At least one of the processors on the local node can communicate with at least one processor on the remote node over the Y fabric. Down: No processor on the local node can communicate with any processor on the remote node over the Y fabric. Unknown: The state of the connection cannot be determined.
Expand Node Number	The Expand node number of the local node. Value: 0 through 254
ServerNet Node Number	The ServerNet node number of the local node. Value: 1 through 96
X Fabric Connection State	The state of the connection from the local node to the remote node over the external ServerNet X fabric. Up: At least one of the processors on the local node can communicate with at least one processor on the remote node over the X fabric. Down: No processor on the local node can communicate with any processor on the remote node over the X fabric. Unknown: The state of the connection cannot be determined.

Expand-Over-ServerNet Configuration

Connectivity State	The state of the Expand-over-ServerNet connection from the local node to the remote node. Values: Connected, Not Connected
Line LDEV Name	The name assigned to the Expand-over-ServerNet line configured from the local node to the selected remote node. Example: \$SC212
Line LDEV	The logical device (LDEV) number of the Expand-over-ServerNet line configured from the local node to the selected remote node. Example: 121
Line LDEV State	The state of the Expand-over-ServerNet line configured from the local node to the selected remote node. Values: Up, Down, Not Available
Remote Line LDEV State	The state of the Expand-over-ServerNet line configured from the remote node to the local node. Values: Up, Down, Unknown

Actions

Generate ServerNet Statistics

Generates an event containing the ServerNet statistics from the local node to the remote node.

ServerNet II Switch

The component of the [6770 switch module](#) that provides routing for the cluster over an external ServerNet fabric. The ServerNet II switch connects to the nodes through fiber-optic cables that connect to plug-in cards on each node.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch

Example: Switch \$ZZSMN.Y1

Attributes

Switch

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

GUID	A unique, read-only number stored in nonvolatile memory (EEPROM) on a ServerNet II switch. The Globally Unique ID can be used programmatically to identify the switch.
Fabric Setting	Whether a switch is configured for operation on the X fabric or the Y fabric. Values: X, Y, or Clear

Firmware

Version	The version of the firmware currently loaded on the switch. The attribute value includes the VPROC string with the firmware version in parentheses. You can also obtain this value from SCF. Example: T0569G06^06MAY02^FMW^AAF (3_0_82)
Default File Name	The name of the file to be used for a firmware update.
Default File Version	The version of the firmware to be used for a firmware update.
Compare State	The differences, if any, between the current and default firmware versions. Values

Configuration

Configuration Tag	A parameter used by SCF and the guided procedures that allows SANMAN to select an appropriate switch configuration block (SCB) from the M6770CL switch configuration library. The selected SCB is subsequently loaded on the specified switch. The configuration tag determines the position of the cluster switch in the topology and the ServerNet node numbers supported by the cluster switch. Values Example: Max 24 nodes, nodes 17-24
Version	The version of the configuration currently loaded on the switch. The attribute value includes the VPROC string with the configuration version in parentheses. You can also obtain this value from SCF. Example: T0569G06^02Jul01^CL4^AAE (2_5)
Default File Name	The full path name of the default configuration file M6770CL.
Position ID	A number that indicates the position that the switch occupies in a network topology. The Position ID is a component of the switch name. For example, the switch name X3 indicates that the switch serves the external ServerNet X fabric and occupies position 3 in the topology.
Default File Version	The version of firmware in the default configuration file M6770CL.
Compare State	The differences, if any, between the current and default configuration versions. Values

Actions

Blink LED Off

Turns off the blinking of the LED.

SCF Equivalent: SCF ALTER SWITCH \$ZZSMN, NEAREST { X | Y}, BLINK NONE

Blink LED On

Causes the LED to start blinking.

SCF Equivalent: SCF ALTER SWITCH \$ZZSMN, NEAREST { X | Y}, BLINK ALL

Configuration Update

This action updates the configuration for the ServerNet II switch component of the 6770 switch module. For more information, see [Updating Cluster Switches](#).

NOTE: If you are updating both firmware and configuration on the same cluster switch, you should always update the firmware first. In some circumstances, updating both firmware and configuration is not necessary. For more information, see the *ServerNet Cluster Manual*.

Optional Parameter: File name of the configuration file.

Firmware Update

Updates the firmware on the ServerNet II switch component of the 6770 switch module. For more information, see [Updating Cluster Switches](#).

Optional Parameter: File name of the firmware file.

Hard Reset

Is necessary following a Configuration Update action in order for the changes to take effect.



CAUTION: This action disrupts the ServerNet traffic through this switch.

SCF Equivalent: SCF RESET SWITCH \$ZZSMN, NEAREST { X | Y }, HARD

Prepare to Replace

Must be performed from each node of a ServerNet cluster before replacing a ServerNet II Switch for SANMAN to accept the new switch.

Replace

Launches the guided procedure for replacing a ServerNet II Switch.

Set Fabric Setting

Sets the fabric LED indicator for the ServerNet II Switch to either X or Y.

Within three minutes after the action completes, the SANMAN process running on each of the nodes discovers that the fabric setting has been corrected and accepts the new switch.

Parameter: Fabric Setting can be set to Unknown, Clear, X, or Y.

SCF Equivalent: SCF ALTER SWITCH \$ZZSMN, NEAREST { X | Y }, FABRIC { X | Y }

Soft Reset

Used following a Firmware Update action on the switch for the changes to take effect.

SCF Equivalent: SCF RESET SWITCH \$ZZSMN, NEAREST { X | Y }, SOFT

Switch Fan

A component that circulates air into the enclosure to help maintain optimal temperature.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch Fan

Example: Fan (1020.1.16)

Attributes

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

LED State	The state of the fault LED on the fan. Values: On, Off, Blinking
Presence	Whether the fan is installed and responding. Values: Present, Absent, Unknown

Logical

Enabled State	The initial state of the component at the time of discovery. Enabled: The component is operational. Disabled: The component is present but not operational, possibly because the Disable action was performed.
Device State	Indication of whether the fan has a fault. Values: OK, Fault

Actions

Blink LED Off

Turns off the blinking of the fault LED.

Blink LED On

Causes the fault LED to start blinking.

Switch Group

A collection of up to four [6780 switches](#) connected together, typically mounted in a rack, that reside on one fabric of a cluster switch zone. The switch group is identified by a four-digit number. The first two digits (10) distinguish a switch group from a group within a NonStop S-series server. The third digit represents the zone number of the switch group, and the fourth digit indicates the external ServerNet fabric where the switch group is located (0 for the X fabric and 1 for the Y fabric).

Location in OSM tree: External ServerNet Fabric > Switch Group

Example: Switch Group 1020 (The switch group in zone 2 on the X fabric)

Attributes

Switch Group

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Presence	Whether the switch group is installed and responding. Values: Present, Absent, and Unknown
----------	--

Actions

None.

Switch Logic Board

A circuit board that provides switching logic for the [6780 switch](#). The logic board connects to a panel on the front of the 6780 switch for operator and maintenance functions.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch Logic Board

Example: Switch Logic Board (1020.1.14)

Attributes

Switch Logic Board

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Hardware Revision	The hardware revision of the switch logic board.
LED State	The state of the fault LED on the switch logic board. Values: On, Off, Blinking
Part Number	The part number of the switch logic board.
Track ID	The track ID of the switch logic board.

Logical

Last Reset Type	The reason for last reset operation. Values: Hardware initiated Soft reset button pressed Front panel button pressed Second Level Watchdog timer expiration Third Level Watchdog timer expiration Firmware initiated Soft reset command issued Hard reset command issued
Time of Last Soft Reset	The date and time of the last processor soft reset.
Time of Last Hard Reset	The date and time of the last processor hard reset.
Firmware State	The state of the switch firmware. Values: Active, Updating, In Test, Initializing, Unknown

Firmware

Version	The VPROC of the firmware currently loaded on the switch logic board.
Default File Name	The full path name of the default firmware file on the server.
Default File Version	The version of the firmware in the default firmware file.
Compare State	The differences, if any, between the current and default firmware versions. Values

Configuration

Configuration Tag	A parameter used by SCF and the guided procedures that allows SANMAN to select an appropriate switch configuration block (SCB) from the switch configuration library. The selected SCB is subsequently loaded on the specified switch. The configuration tag determines the position of the cluster switch in the topology and the ServerNet node numbers supported by the cluster switch. Values Example: 9721
Version	The VPROC of the configuration currently loaded on the switch logic board.
Default File Name	The full path name of the default configuration file on the server.
Default File Version	The version of the configuration in the default configuration file.
Compare State	The differences, if any, between the current and default configuration files. Values

FPGA

Version	The VPROC of the FPGA (field programmable gate array) image currently loaded on the switch logic board.
Default File Name	The full path name of the default FPGA file on the server.
Default File Version	The version of the FPGA image in the default FPGA file.
Compare State	The differences, if any, between the current and default FPGA versions. Values

Actions

Blink LED Off

Turns off the blinking of the fault LED.

Blink LED On

Causes the fault LED to blink to make it easier to identify the component.

Configuration Update

Loads a configuration file from the local node to the switch logic board and prompts the user to change the numeric selector to the desired value. For details, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

Optional Parameter: File Name— the name of the configuration file on the local node

Syntax: \$volume.subvolume

Default value: \$SYSTEM.SYSnn

Dump

Copies a memory image from a 6780 switch to a specified file on the local system.

Firmware Update

Loads a firmware file from the local node to the switch logic board. For details, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

Optional Parameter: File Name—the name of the firmware file on the local node

Syntax: \$volume.subvolume

Default value: \$SYSTEM.SYSnn

FPGA Update

Loads an FPGA code file from the local node to the switch logic board. For details, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

Optional Parameter: File Name—the name of the FPGA code file on the local node

Syntax: \$volume.subvolume

Default value: \$SYSTEM.SYSnn

Hard Reset

Hard resets the switch logic board.

SCF Equivalent: RESET SWITCH, HARD

Replace

Invokes the Replace Switch Component guided procedure that helps to replace the switch logic board.

Soft Reset

Soft resets the switch logic board.

SCF Equivalent: RESET SWITCH, SOFT

Switch PIC

A card in the [6780 switch](#) that plugs into the switch logic board. Most switch PICs (except for maintenance PICs and router interconnect PICs) are populated with transceivers that enable connections to the different nodes, layers, and zones of the cluster.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch PIC

Example: Switch PIC \$ZZSMN.Y11.13 (1011.1.13)

See also [Router Connections for Router Interconnect PICs](#).

Attributes

Switch PIC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Model	The type of PIC. Values: Single-mode fiber-optic, Multimode fiber-optic, Router Interconnect, Maintenance, Dual Single-mode fiber-optic, Quad Multimode fiber-optic
Part Number	The part number of the switch PIC.
Presence	Whether the PIC is installed and responding.
LED State	The state of the fault LED on the switch PIC. Values: On, Off, Blinking
Track ID	The track ID of the switch PIC.
Manufacturer	Identifies the manufacturer of the component.
Hardware Revision	The hardware revision of the switch PIC.

Logical

Enabled State	The initial state of the component at the time of discovery. Enabled: The component is operational. Disabled: The component is present but not operational.
Device State	Indication of whether the switch has a fault. Values: OK, Fault

Actions

Blink LED Off

Turns off the blinking of the LEDs.

Blink LED On

Causes the LEDs to start blinking.

Replace

Invokes the Replace Switch Component guided procedure that helps to replace the switch PIC.

Switch Power Supply

A component in the switch modules that converts standard AC line voltage and distributes DC power to all components in the module.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch Power Supply

Example: Power Supply (1010.1.18)

Attributes

Power Supply

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the power supply.
Presence	Whether the Power Supply is installed and responding. Values: Present, Absent, Unknown
LED State	The state of the fault LED on the power supply. Values: On, Off, Blinking
Track ID	The track ID of the power supply.
Manufacturer	Identifies the manufacturer of the component.
Hardware Revision	The hardware revision of the power supply.

Logical

Enabled State	The initial state of the component at the time of discovery. Enabled: The component is operational.
---------------	---

	Disabled: The component is present but not operational.
Device State	Whether the power supply has a fault. Values: OK, Fault

Actions

Blink LED Off

Turns off the blinking of the LEDs.

Blink LED On

Causes the LEDs to start blinking.

Switch-to-Node PIC

A plug-in card (PIC) on the [6770 switch module](#) that connects to a ServerNet node. The last part of the name contains the port number where the PIC is located. Only the PICs in ports 0 through 7 of the switch are used for switch-to-node connections.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch > Switch PIC

Example: Switch PIC \$ZZSMN.X2.4 (indicates the PIC in port 4 of switch X2)

Attributes

Switch PIC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Connectivity Status	The state of connectivity between the switch and the node to which this PIC connects. Values: Connected Not Connected Connected to Switch With Wrong Fabric Connected to Node Connected to Wrong Port Connected to Different Switch Connected to Switch With Wrong Configuration Unknown
Presence	Whether the PIC is installed and responding. Values: Present, Absent, Unknown
Fabric State	The state of the external ServerNet fabric from the local node to the remote node connected via this port. Values

Neighbor ServerNet Node

Node Name	The neighbor node to which this PIC is connected. Example: ServerNet Local Node \STAR1
Node Number	The ServerNet node number of the neighbor node to which this PIC is connected.

Actions

Node Responsive Test

Tests the connectivity on the external ServerNet fabric through this port.

Switch Node Port

On the [6780 switch](#), an external transceiver port that connects to a ServerNet node. These ports reside only on switch PICs in slots 6 through 9.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch PIC > Switch Port

Example: Switch Port (1010.1.6.1)

See also [Router Connections for Switch Node Ports](#).

Attributes

Switch Node Port

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Transceiver Physical

Type	The type of transceiver. Example: 9/125 Micron SMF
Part Number	The vendor part number of the transceiver.
Serial Number	The vendor serial number of the transceiver.
Manufacturer	Identifies the manufacturer of the component.
Hardware Revision	The vendor hardware revision of the transceiver.

Logical

Connectivity Status	The status of the port. Values: Port reset Loss of optical signal Transceiver absent PIC absent No link alive Link Alive - Port disabled Neighbor check in progress Neighbor check complete - Port disabled Neighbor check failed - No link alive Connected to switch Connected to switch with wrong numeric selector Connected to switch with invalid configuration version identifier Connected to wrong port Connected to different switch Connected to switch with incompatible configuration No response to Manage Port command from neighbor port Manage Port command not acknowledged (NACKed) from neighbor port Port enabled Invalid Unknown
Current Speed	The speed of the port in bits per second.

Transceiver Device State	The initial state of the component at the time of discovery. Values: OK, Fault
Transceiver Enabled State	Whether the transceiver is enabled. Enabled: The component is operational. Disabled: The component is present but not operational.
Fabric State	The state of the external ServerNet fabric from the local node to the remote node connected via this port. Up: At least one of the processors on the local node can communicate with at least one processor on one of the remote nodes. Down: No processor on the local node can communicate with any processor on any remote node.

Neighbor ServerNet Node

Node Number	The ServerNet node number of the neighbor node.
Node Name	The name of the neighbor node.

Actions

Node Responsive Test

Tests the connectivity on the external ServerNet fabric from the local node to the remote node connected via this port.

Switch-to-Switch PIC

A plug-in card (PIC) on the [6770 switch module](#) that connects to another switch on the same fabric. The last part of the name contains the port number where the PIC is located. Only the PICs in ports 8 through 11 of the switch are used for switch-to-switch connections.

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch > Switch PIC

Example: Switch PIC \$ZZSMN.Y3.10 (indicates the PIC in port 10 of switch Y3)

Attributes

Switch PIC

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Logical

Connectivity Status	The state of connectivity between the switch and the node to which this PIC connects. Values: Connected Not Connected Connected to Switch With Wrong Fabric Connected to Node Connected to Wrong Port Connected to Different Switch Connected to Switch With Wrong Configuration
---------------------	---

	Unknown
Presence	Whether the PIC is installed and responding. Values: Present, Absent, Unknown

Neighbor Switch PIC

PIC Name	The neighbor switch and PIC to which this PIC is connected. Example: Switch PIC \$ZZSMN.X.1.8 (indicates that this PIC is connected to switch X1, PIC 8)
----------	--

Actions

None.

Switch Port

An external transceiver port on a [6780 switch](#) that connects to a 6780 switch in another zone or layer. These ports reside only on switch [PICs](#) in slots 2 and 3 (for zone connections) and 11 through 13 (for layer connections).

Location in OSM tree: External ServerNet Fabric > Switch Group > Switch Module > Switch PIC > Switch Port

Example: Switch Port (1010.1.13.4)

See also [Router Connections for Ports Connecting to Other Switches](#).

Attributes

Switch Port

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Transceiver Physical

Type	The type of transceiver. Example: 50/125 - 62.5/125 Micron MMF
Part Number	The vendor part number of the transceiver.
Serial Number	The vendor serial number of the transceiver.
Manufacturer	Identifies the manufacturer of the component.
Hardware Revision	The vendor hardware revision of the transceiver.

Logical

Connectivity Status	The status of the port. Values: Port reset Loss of optical signal Transceiver absent PIC absent No link alive Link Alive - Port disabled Neighbor check in progress Neighbor check complete - Port disabled Neighbor check failed - No link alive
---------------------	--

	Connected to node Connected to switch with wrong numeric selector Connected to switch with invalid configuration version identifier Connected to wrong port Connected to different switch Connected to switch with incompatible configuration No response to Manage Port command from neighbor port Manage Port command not acknowledged (NACKed) from neighbor port Port enabled Invalid Unknown
Current Speed	The speed of the port in bits per second.
Transceiver Device State	The initial state of the component at the time of discovery. Values: OK, Fault
Transceiver Enabled State	Whether the transceiver is enabled. Enabled: The component is operational. Disabled: The component is present but not operational.

Neighbor Switch Port

Switch Port	The name of the port to which this port is connected. Format: Port (Group.Module.Slot.Port) where: Group can be 1010, 1020, 1030, 1011, 1021 or 1031. Module can be 1, 2, 3 or 4. Slot can be 2, 3, 11, 12 or 13. Port can be 1, 2, 3 or 4.
-------------	--

Actions

None.

UPS (6770 Switch Module)

The uninterruptible power supply (UPS) is a component of a [6770 switch module](#) that provides two hours of power if both the primary and backup AC power sources fail.

Location in OSM tree:External ServerNet Fabric > Switch Group > Switch Module > UPS

Example:UPS \$ZZSMN.X1

Attributes

UPS

Service State	Displayed in the Attributes tab and Attributes dialog box only if the value is something other than OK. Values
---------------	--

Physical

Part Number	The part number of the UPS.
Track ID	A unique serial number that identifies the component. Track IDs are used for tracking components.
Type	The VA rating (volts multiplied by amps) and the firmware version of the UPS. Example: UPS 1440 VA FW -0039

Logical

Estimated Charge Remaining	The percentage of charge remaining in the UPS batteries.
Remaining Time	The amount of time remaining (in minutes) that the UPS battery will provide power to the switch in the event that both the primary and backup rails lose power, or if the input voltage of the AC power source is not within the allowable range.
Remaining Capacity Status	The remaining capacity level in the UPS batteries. Values: Normal, Low, Depleted If the value is Depleted, the UPS is unable to sustain the present load if utility power is lost or absent.

Actions

Replace

Launches the Replace Switch Component guided procedure, which provides help for replacing the component.

Common Attribute Values

Service State

This attribute appears in the list of attributes only when attention or service is required.

Value	Meaning
OK	The object is functioning properly. This value appears only in the Problem Summary dialog box.
Attention Required	The resource requires operator attention. This condition sometimes generates an alarm, and the component that requires attention is colored yellow in the tree pane and in the Physical and ServerNet views of the view pane.
Service Required	The resource requires service. This condition generates an alarm, and the component that requires service is colored red in the tree pane and in the Physical and ServerNet views of the view pane.

Fabric State

Value	Meaning
Up	At least one of the processors on the local node can communicate with at least one processor on one of the remote nodes.
Down	No processor on the local node can communicate with a processor on any remote node. This value is the default. NOTE: The Fabric state for a one-node ServerNet cluster is Down because communication with processors in remote nodes is not possible.

Configuration Tag

This table shows the supported configuration tags for each topology:

Topology	Supported Configuration Tags*	OSM and Guided Procedures Display Value
N/A	0x11111 (manufacturing default)	0x11111
Star	0x10000	Max 8 nodes, nodes 1-8 (0x10000)

Topology	Supported Configuration Tags*	OSM and Guided Procedures Display Value
Split-star	0x10000	Max 16 nodes, nodes 1-8 (0x10000)
	0x10001	Max 16 nodes, nodes 9-16 (0x10001)
Tri-star	0x10002	Max 24 nodes, nodes 1-8 (0x10002)
	0x10003	Max 24 nodes, nodes 9-16 (0x10003)
	0x10004	Max 24 nodes, nodes 17-24 (0x10004)

Port Connectivity Status

Value	Valid Only For
Reset	
Link dead (Loss of optical signal)	
Link dead (Transceiver absent)	
No link alive	
Link alive, port disabled	
Link alive, port disabled, neighbor check in progress	
Link alive, port disabled, neighbor check complete	
Link alive, port disabled, neighbor check failed (Not connected)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to switch)	Switch-to-Node Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to node)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to switch with invalid configuration version identifier)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to switch with incompatible configuration)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to switch with wrong numeric selector)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to wrong port)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port disabled, neighbor check failed (Connected to different switch)	Zone-to-Zone Interconnect and Layer-to-Layer Interconnect ports
Link alive, port enabled	

14 Updating ServerNet Cluster Topology

You can update a ServerNet cluster to support more nodes or to expand the geographical limits of the cluster.

These topics provide guidance on the different types of topology updates:

- To locate relevant information for your update, see [Identifying Your Update Type](#).
- If you need to add a node to a cluster without changing the topology, log on to the node using OSM, and perform the [Add Node to ServerNet Cluster](#) action. This action launches a guided procedure with online help to assist you.

Identifying Your Update Type

These topics describe different ways to update a ServerNet cluster. Click the appropriate link for your type of update.

- [Migrating to the Layered Topology](#) describes how to migrate a cluster from one of the star topologies to the layered topology.
- [Adding Zones or Layers to a Layered Topology](#) describes how to add zones or layers to a cluster already using the layered topology.
- [Updating Star Topologies](#) describes how to use the OSM Update ServerNet Cluster Topology action to:
 - Merge two star topologies to create a split-star topology
 - Merge a star topology and a split-star topology to create a tri-star topology
 - Merge three star topologies to create a tri-star topology

Migrating to the Layered Topology

The layered topology requires HP NonStop ServerNet Switches (model 6780).

To migrate a ServerNet cluster from one of the star topologies to the layered topology, you must have on hand enough 6780 switches and ServerNet cables to support your cluster. You need at least two switches (one for each external fabric) for every eight nodes.

For details on planning a migration to the layered topology, including hardware, software, and cabling requirements, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

For a quick reference on cable connections, see [Cable Connections in a Layered Topology](#).

Adding Layers or Zones to a Layered Topology

You can expand an existing ServerNet cluster that uses the layered topology by adding layers or zones.

For complete instructions for adding layers or zones, see the *ServerNet Cluster 6780 Planning and Installation Guide*.

Updating Star Topologies

Follow this procedure only if you plan to use OSM to merge clusters to create a split-star or tri-star topology.

These three methods are supported for updating to the split-star or tri-star topology:

- Merging two star topologies to create a split-star topology
- Merging a star topology with a split-star topology to create a tri-star topology
- Merging three star topologies to create a tri-star topology

The major steps in updating a topology are:

1. Review the planning information in the *ServerNet Cluster Manual* for your type of update. Decide which nodes will be connected to each pair of switches in the new topology by using the planning forms in the manual.
2. Ensure you have all the cluster switches and ServerNet cables in place to expand your cluster. For complete hardware requirements, see the *ServerNet Cluster Manual*.
3. Ensure that at least one node is connected to each cluster switch.
4. Ensure you have the minimum levels of software running on all the nodes of your cluster. Because you are using OSM to perform the update, you might already have newer versions of the software described in the manual. Even so, be sure all nodes meet the minimum requirements described in [Software Requirements for Split-Star and Tri-Star Topologies](#).
5. Ensure that you have the minimum version of firmware and configuration on each cluster switch. See [Software Requirements for Split-Star and Tri-Star Topologies](#).

⚠ CAUTION: Do not proceed if you have the T0569AAA configuration running on any of the switches. Doing so can cause outages on every system in the cluster.

6. Use the OSM service connection to ensure that the clusters to be merged are trouble free. If there are any alarms, follow the repair actions to resolve the problems.
7. Use the Configuration Update action to change the configuration tags so they are compatible with the new topology:
 - If you are merging two star topologies to create a split-star topology, change the configuration tags for the switches in one star topology to support node numbers 9 through 16.
 - If you are merging a split-star topology with a star topology to create a tri-star topology, change the configuration tags for the switches in the star topology to support node numbers 17 through 24. This practice avoids the need for a configuration tag change on the split-star topology. (The split-star topology already uses node numbers 1 through 16.)
 - If you are merging three star topologies to create a tri-star topology, change the configuration tags for the switches in one star topology to support node numbers 9 through 16. Change the configuration tags for the switches in another star topology to support node numbers 17 through 24. (The remaining star topology should already use node numbers 1 through 8.)

NOTE: Changing the configuration tag requires a hard reset of the switches, resulting in a temporary disruption of ServerNet connectivity. After the configuration tags match on respective X and Y switches, the connectivity is repaired.

8. Perform the Update Topology action on each cluster. When prompted, click the Disable Cluster Alarms button. No alarms related to connectivity (that would otherwise be dialed out on multiple nodes) are dialed out for two hours unless you perform the Rediscover action. Other types of alarms, such as hardware failures, are still dialed out.
9. Disconnect any existing X-fabric cables between the cluster switches. (If you are updating from a star topology, there are no existing cables between switches.)
10. Connect all the cables between the X-fabric switches to support the new topology. The new switch port connections will differ from the original cluster. See [Cable Connections Between Star Groups](#). For more information on connecting cables refer to the *ServerNet Cluster Manual*.

11. Use OSM to monitor the connectivity on the X fabric for all the nodes and switches. Connectivity on the X fabric should be restored over time. Confirm that the original nodes of the cluster are visible. If necessary, resolve any connectivity problems by following the repair actions.
12. Disconnect any existing Y-fabric cables between the cluster switches. (If you are updating from a star topology, there are no existing cables between switches.)
13. Connect all the cables between the Y-fabric switches to support the new topology. The new switch port connections will differ from the original cluster. See [Cable Connections Between Star Groups](#). For more information on connecting cables, refer to the *ServerNet Cluster Manual*.
14. Use OSM to monitor the connectivity on the Y fabric for all the nodes and switches. Connectivity on the Y fabric should be restored over time. Confirm that the nodes from the original clusters are visible.
15. If any nodes are not visible to the cluster, perform the Add Node to ServerNet Cluster action on the nodes that are not visible to the cluster.
16. If there are no connectivity problems, perform the Rediscover action on the ServerNet Cluster resource. OSM is now configured to dial out alarms.

If you need to add new nodes to the cluster, use the [Add Node to ServerNet Cluster](#) action. This action launches a guided procedure with online help to assist you.

If you need to move any nodes within the cluster, see the information on moving a node in the *ServerNet Cluster Manual*.

Software Requirements for Split-Star and Tri-Star Topologies

Any node that will participate in a ServerNet cluster must have Expand (T9057) software, which is delivered on the site update tape (SUT). In addition, the Expand/ServerNet Profile (T0569) is required for clustering. If you order the optional Expand/ServerNet Profile component, it is delivered on the SUT.

Additional software requirements depend on the topology you use to construct the ServerNet cluster:

Software Component	Split-Star Topology	Tri-Star Topology
Operating system	G06.09 or later (G06.09, G06.10, and G06.11 require SPRs)	G06.13 or later (G06.13 requires SPRs)
SNETMON/ MSGMON	Depends on operating system. For compatibility information, see the SNETMON/MSGMON softdoc.	Depends on operating system. For compatibility information, see the SNETMON/MSGMON softdoc.
SANMAN	T0502AAE or superseding	T0502AAG or superseding
Switch Firmware and Configuration	T0569AAB or superseding	T0569AAE or superseding
OSM Client	T2752AAB or superseding	T2752AAB or superseding
OSM Server	G06.21 or later (Server components should be AAB or superseding.)	G06.21 or later (Server components should be AAB or superseding.)
SP firmware	T1089ABB or superseding	T1089ABC or superseding
SCF	T9082ACQ or superseding	T9082ACQ or superseding

Cable Connections Between Star Groups

Updating to the Split-Star Topology

If you are updating to the split-star topology, connect the cables as follows:

Cluster Switch	Port	Connects to Cluster Switch	Port
X1	8	X2	8
X1	9	X2	9
X1	10	X2	10
X1	11	X2	11
Y1	8	Y2	8
Y1	9	Y2	9
Y1	10	Y2	10
Y1	11	Y2	11

Updating to the Tri-Star Topology

If you are updating to the tri-star topology, connect the cables as follows:

Cluster Switch	Port	Connects to Cluster Switch	Port
X1	8	X2	10
X1	9	X2	11
X1	10	X3	8
X1	11	X3	9
X2	8	X3	10
X2	9	X3	11
Y1	8	Y2	10
Y1	9	Y2	11
Y1	10	Y3	8
Y1	11	Y3	9
Y2	8	Y3	10
Y2	9	Y3	11

Cable Connections in a Layered Topology

Connections Between Layers Within a Switch Group

This table lists the connections between layers within a switch group:

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X11/Y11	11	1	X12/Y12	11	1
X11/Y11	11	2	X12/Y12	11	2
X11/Y11	11	3	X12/Y12	11	3

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X11/Y11	11	4	X12/Y12	11	4
X11/Y11	12	1	X13/Y13	12	1
X11/Y11	12	2	X13/Y13	12	2
X11/Y11	12	3	X13/Y13	12	3
X11/Y11	12	4	X13/Y13	12	4
X11/Y11	13	1	X14/Y14	13	1
X11/Y11	13	2	X14/Y14	13	2
X11/Y11	13	3	X14/Y14	13	3
X11/Y11	13	4	X14/Y14	13	4
X12/Y12	12	1	X14/Y14	12	1
X12/Y12	12	2	X14/Y14	12	2
X12/Y12	12	3	X14/Y14	12	3
X12/Y12	12	4	X14/Y14	12	4
X12/Y12	13	1	X13/Y13	13	1
X12/Y12	13	2	X13/Y13	13	2
X12/Y12	13	3	X13/Y13	13	3
X12/Y12	13	4	X13/Y13	13	4
X13/Y13	11	1	X14/Y14	11	1
X13/Y13	11	2	X14/Y14	11	2
X13/Y13	11	3	X14/Y14	11	3
X13/Y13	11	4	X14/Y14	11	4

X Fabric Connections Between Two Zones

This table lists the X-fabric connections between two zones of a layered topology.

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X11	2	1	X21	2	2
X11	2	2	X21	2	1
X11	3	1	X21	3	2
X11	3	2	X21	3	1
X12	2	1	X22	2	2
X12	2	2	X22	2	1
X12	3	1	X22	3	2
X12	3	2	X22	3	1
X13	2	1	X23	2	2
X13	2	2	X23	2	1
X13	3	1	X23	3	2
X13	3	2	X23	3	1

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X14	2	1	X24	2	2
X14	2	2	X24	2	1
X14	3	1	X24	3	2
X14	3	2	X24	3	1

Y Fabric Connections Between Two Zones

This table lists the Y-fabric connections between two zones of a layered topology:

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
Y11	2	1	Y21	2	2
Y11	2	2	Y21	2	1
Y11	3	1	Y21	3	2
Y11	3	2	Y21	3	1
Y12	2	1	Y22	2	2
Y12	2	2	Y22	2	1
Y12	3	1	Y22	3	2
Y12	3	2	Y22	3	1
Y13	2	1	Y23	2	2
Y13	2	2	Y23	2	1
Y13	3	1	Y23	3	2
Y13	3	2	Y23	3	1
Y14	2	1	Y24	2	2
Y14	2	2	Y24	2	1
Y14	3	1	Y24	3	2
Y14	3	2	Y24	3	1

X Fabric Connections for Three Zones

This table lists the X-fabric connections for three zones of a layered topology:

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X11	2	1	X21	2	2
X11	2	2	X31	2	1
X11	3	1	X21	3	2
X11	3	2	X31	3	1
X12	2	1	X22	2	2
X12	2	2	X32	2	1
X12	3	1	X22	3	2
X12	3	2	X32	3	1

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
X13	2	1	X23	2	2
X13	2	2	X33	2	1
X13	3	1	X23	3	2
X13	3	2	X33	3	1
X14	2	1	X24	2	2
X14	2	2	X34	2	1
X14	3	1	X24	3	2
X14	3	2	X34	3	1
X21	2	1	X31	2	2
X21	3	1	X31	3	2
X22	2	1	X32	2	2
X22	3	1	X32	3	2
X23	2	1	X33	2	2
X23	3	1	X33	3	2
X24	2	1	X34	2	2
X24	3	1	X34	3	2

Y Fabric Connections for Three Zones

This table lists the Y-fabric connections for three zones of a layered topology:

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
Y11	2	1	Y21	2	2
Y11	2	2	Y31	2	1
Y11	3	1	Y21	3	2
Y11	3	2	Y31	3	1
Y12	2	1	Y22	2	2
Y12	2	2	Y32	2	1
Y12	3	1	Y22	3	2
Y12	3	2	Y32	3	1
Y13	2	1	Y23	2	2
Y13	2	2	Y33	2	1
Y13	3	1	Y23	3	2
Y13	3	2	Y33	3	1
Y14	2	1	Y24	2	2
Y14	2	2	Y34	2	1
Y14	3	1	Y24	3	2
Y14	3	2	Y34	3	1
Y21	2	1	Y31	2	2

Switch	PIC Slot	Port	Connect to Switch	PIC Slot	Port
Y21	3	1	Y31	3	2
Y22	2	1	Y32	2	2
Y22	3	1	Y32	3	2
Y23	2	1	Y33	2	2
Y23	3	1	Y33	3	2
Y24	2	1	Y34	2	2
Y24	3	1	Y34	3	2

Index

Symbols

4PSE, 78

- actions, 78
- attributes, 78

6770 Switch Module

- about, 254
- actions, 255
- attributes, 255

6780 Switch Module

- about, 255
- actions, 256
- attributes, 255

A

AC Transfer Switch

- about, 257
- actions, 257
- attributes, 257

Access Control List, 66

actions

- automatically initiating, 68
- controlling access, 66
- detailed information about, 68
- on multiple resources, 69
- performing, 66
- performing on a resource, 68
- saving details, 71
- stopping, 68
- summary of, 74
- viewing details, 71

Add Node to ServerNet Cluster, 223, 225

Alarm Panel

- about, 79
- actions, 80
- attributes, 79

alarms

- deleting, 63, 74
- detailed information, 74
- details of, 62
- finding, 74
- printing information, 62
- saving information, 62
- sorting, 74
- summary of, 74
- suppressing, 63, 74
- viewing, 61

ATM Adapter CRU

- about, 80
- actions, 81
- attributes, 80

ATM Line

- about, 82
- attributes, 82

ATM3SA see ATM Adapter CRU

attributes

- actions for, 64
- in Details pane, 64
- printing, 64
- saving, 64
- seeing description, 64
- suppressing, 64
- using dialog box, 64
- viewing, 64

Automatic Data Collection State, 222

automatically create Client Certificate,

B

Backup CLIM Configuration action, 98

Battery

- about, 83
- actions, 84
- attributes, 83

Blade Complex

- about, 84
- actions, 85
- attributes, 84

Blade Element

- about, 85
- actions, 87
- attributes, 86

Blade Element Firmware

- about, 90
- attributes, 90

Blade System Board

- about, 92

BladeCluster

- about, 257
- actions, 258
- attributes, 258

BladeCluster Solution, 249

Blink LED Off, 266

Blink LED On, 267

Blower (FCDM)

- about, 92
- actions, 93
- attributes, 93

Bring Up and Balance Storage Paths, 223

C

CCSA CRU

- about, 93
- actions, 94
- attributes, 93

certification method, selecting,

Check DHCP and DNS Server Status, 223

Check Storage Dependence on ServerNet Fabric, 223

Clear External BladeCluster Configuration, 223

CLIM, 94

CLIM username and password, creating,

CLIM-Attached Disk

- about, 108

- CLIM-Attached Disks, [102](#)
- CLIMs, [133](#)
- CLIMs (container object), [99](#)
- Cluster
 - about, [262](#)
 - actions, [263](#)
 - attributes, [262](#)
- cluster of Key Managers,
- cluster resources
 - list of, [254](#)
 - locating, [249](#)
 - managing, [254](#)
 - monitoring, [250](#)
 - performing actions on, [250](#)
 - viewing, [249](#)
- cluster switch
 - specifying location, [251](#)
- cluster topology
 - updating, [280](#)
- CMAP, reinitialize, [226](#)
- Collect CLIM Logs, [100](#)
- Collect CLIM Logs action, [98](#)
- Collect Diagnostic Data, [224](#)
- Common Communication ServerNet Adapter see CCSA CRU
- Compare HSS Firmware Versions, [224](#)
- Configuration Update, [267](#), [270](#)
- Configure CLIM action, [100](#)
- configure Key Manager Cluster,
- connectivity check,
- Copy Core License to Alternate System Disk, [224](#)
- cut and paste certificate,

D

- Data Sanitization, [226](#)
- Days to Persist Collected Diagnostic Data, [222](#)
- define tiers,
- delete NSSuser,
- Delete System Load Configuration, [224](#)
- Detect New Hardware, [224](#)
- Diagnostic Data Collection Volume, [222](#)
- DIMM, [103](#)
- Disk
 - ESS, [122](#)
 - External, [125](#)
 - Fibre Channel, [111](#)
 - SAS, [116](#)
- Disk (Fibre Channel)
 - about, [111](#)
 - actions, [113](#)
 - attributes, [112](#)
- Disk CRU
 - about, [103](#)
 - actions, [105](#)
 - attributes, [103](#)
- Disk Name, [223](#)
- Down System CLIM Firmware Update Tool, [100](#)
- Dump, [270](#)
- DVD-ROM

- about, [117](#)

E

- E4SA CRU
 - about, [118](#)
 - actions, [118](#)
 - attributes, [118](#)
- EMU
 - about, [119](#)
 - actions, [119](#)
 - attributes, [119](#)
- Enable/Disable Automation of Data Collection, [224](#)
- Enable/Disable Blade Power Regulator Management, [224](#)
- Enclosure, [120](#)
- Enterprise Storage System Disk drive, [122](#)
- ESS Disk
 - about, [122](#)
 - actions, [109](#), [124](#)
- ESS Disk Collection
 - about, [125](#)
- Ethernet 4 ServerNet Adapter see E4SA CRU
- Extend Problem Incident Report Suppression Time, [225](#)
- External Disk
 - about, [125](#)
 - actions, [127](#)
 - attributes, [126](#)
- External Disk Collection
 - about, [129](#)
- external fabric
 - about, [259](#)
 - actions, [259](#)
 - attributes, [259](#)
- External ServerNet Fabric
 - about, [259](#)

F

- Fan
 - about, [129](#)
 - actions, [130](#)
 - attributes, [130](#)
 - for IOAM, [131](#)
 - for VIO module, [133](#)
- Fan (Processor Switch)
 - about, [132](#)
 - actions, [132](#)
 - attributes, [132](#)
- Fan Assembly (Blade Element)
 - about, [130](#), [131](#)
- Fast Ethernet ServerNet Adapter
 - about, [143](#)
- FC-AL I/O Module
 - about, [134](#)
 - actions, [135](#)
 - attributes, [134](#)
- FCDM
 - about, [135](#)
 - actions, [137](#)
 - attributes, [120](#), [136](#)
- FCDM Collection

- about, [138](#)
- attributes, [138](#)
- FCSA
 - about, [138](#)
 - actions, [139](#), [235](#)
 - attributes, [139](#), [234](#)
 - removing and installing, [140](#)
- FCSA FSAC
 - about, [142](#)
 - actions, [143](#)
 - attributes, [142](#)
- FESA
 - about, [143](#)
 - actions, [143](#)
 - attributes, [143](#)
- Fiber, [144](#)
- Fiber ServerNet Addressable Controller *see* FSAC
- Fibre Channel Router
 - about, [144](#)
 - actions, [145](#)
 - attributes, [144](#)
- firmware
 - updating, [76](#)
- Firmware update
 - Switch Logic Board, [270](#)
- firmware updates
 - performing, [71](#)
- FPGA code update
 - Switch Logic Board, [271](#)
- FSAC, [113](#)
 - about, [145](#)
 - actions, [146](#)
 - attributes, [146](#)

G

- G4SA
 - about, [146](#)
 - actions, [147](#)
 - attributes, [146](#)
- G4SA PIF
 - about, [147](#)
 - actions, [148](#)
 - attributes, [148](#)
- G4SA SAC
 - about, [149](#)
 - actions, [150](#)
 - attributes, [149](#)
- Generate ServerNet Statistics, [261](#)
- GESA CRU
 - about, [150](#)
 - actions, [151](#)
 - attributes, [151](#)
- Gigabyte Ethernet ServerNet Adapter *see* GESA CRU
- Group (IOAM or Fabric)
 - actions, [153](#)
 - attributes, [153](#)
- Group (IOAM, Fabric, G16SE)
 - about, [153](#)
- Group (IOMF2 Enclosure or Processor Group)

- actions, [152](#)
- attributes, [152](#)
- Group (IOMF2 or VIO)
 - about, [152](#)

H

- Halt Code, [162](#)
- Halt Flag, [162](#)
- Hard Disk (CLIM), [154](#)
- Hard Reset, [267](#), [271](#)
- HP SIM, [44](#)
- hung system or processor, recovery, [228](#)

I

- I/O Multifunction 2 CRU *see* IOMF2 CRU
- Infiniband HCA Card, [154](#)
- Initialize Default Firmware File Names, [225](#)
- Install Core License File, [226](#)
- internal fabric
 - about, [155](#)
 - actions, [156](#)
 - attributes, [156](#)
- Internal ServerNet Fabric
 - about, [155](#)
- IO Module, [156](#)
- IOAM
 - about, [156](#)
 - actions, [157](#)
 - attributes, [157](#)
- IOAM Enclosure
 - about, [157](#)
 - actions, [158](#)
 - attributes, [158](#)
- IOAM Fan
 - actions, [132](#)
 - attributes, [132](#)
- IOMF2 CRU
 - about, [159](#)
 - actions, [160](#)
 - attributes, [159](#)

L

- LIF
 - about, [161](#)
 - actions, [161](#)
 - attributes, [161](#)
- Local CA that signed server certificate,
- Local CA to sign client certificates,
- Local Node
 - about, [264](#)
 - actions, [264](#)
 - attributes, [264](#)
- Local or Remote BladeCluster Node
 - about, [259](#)
 - actions, [261](#)
- Logical Processor
 - about, [162](#)
 - actions, [163](#)
 - attributes, [162](#)

Logical Processor State, [162](#)

M

Maintenance PIC

about, [165](#)

actions, [165](#)

attributes, [165](#)

Maintenance Switch

about, [165](#)

actions, [166](#)

attributes, [165](#)

managing a system, [76](#)

Memory Card

about, [166](#)

Module

about, [167](#)

actions, [168](#)

attributes, [167](#)

Monitored Service LAN Devices

about, [169](#)

actions, [169](#)

Motherboard, [169](#)

N

NIC, [170](#)

Node Connectivity ServerNet Path Test, [259](#)

Node Responsive Test, [274](#), [275](#)

NonStop Setup User Credentials,

NSSuser, deleting,

NSSuser, enter credentials,

O

Optical Extender PIC, [171](#)

actions, [172](#)

attributes, [171](#)

P

PCI Riser, [172](#)

PE Blade Element Track ID, [189](#)

PE LID, [189](#)

PE Memory Size, [189](#)

PE Reintegration Enable State, [189](#)

PE State, [190](#)

PE Stop Code, [190](#)

Perform Data Sanitization, [226](#)

Physical Configuration Tool, [72](#)

PIC

about, [172](#)

actions, [173](#)

attributes, [172](#)

PIC Model, [271](#)

PIF

about, [174](#)

actions, [175](#)

attributes, [174](#)

Place Local Node in Service, [258](#)

PMCU

about, [175](#)

attributes, [175](#)

Power Supply

about, [176](#)

actions, [177](#)

attributes, [176](#)

replacement guidelines, [177](#)

Power Supply (Blade Element)

about, [180](#)

actions, [181](#)

attributes, [180](#)

Power Supply (CLIM)

about, [181](#)

attributes, [181](#)

Power Supply (FCDM)

about, [181](#)

actions, [182](#)

attributes, [182](#)

Power Supply (IOAM)

about, [182](#)

attributes, [182](#)

Power Supply (Processor Switch)

about, [184](#)

actions, [184](#)

attributes, [184](#)

Power Supply (VIO module)

about, [185](#)

attributes, [186](#)

power-fail scenarios, [46](#)

configuring Integrity NonStop BladeSystem, [121](#)

configuring Integrity NonStop NS14000 or NS1000
system for, [183](#)

configuring Integrity NonStop NS14000 series,
NS1200, or NS1000 system for, [186](#)

configuring Integrity NonStop NS16000 series server
for, [184](#)

Prepare for Down System CLIM Firmware Update, [100](#)

Prepare to Replace, [267](#)

Problem Incident Report Creation State, [223](#)

Processor

attributes, [188](#)

Processor (CLIM)

about, [187](#)

attributes, [187](#)

Processor Blade

about, [187](#)

Processor Components

about, [189](#)

actions, [191](#)

attributes, [189](#)

Processor Freeze State, [163](#)

processor hang, recovery, [228](#)

Processor State, [163](#)

Processor Switch

about, [192](#)

actions, [193](#)

attributes, [193](#)

Processor Type, [163](#)

R

Read Core License, [226](#)

- Read Core License File, [226](#)
- Rediscover System, [226](#)
- Rediscover System and ServerNet Cluster, [226](#)
- Redundancy State, [163](#)
- Register CLIMs with Key Managers (guided procedure), [102](#)
- register CLIMs, final step,
- Reinitialize Complex Manager, [226](#)
- Remote 6770 Switch
 - about, [261](#)
 - attributes, [261](#)
- Remote Node
 - about, [264](#)
 - actions, [265](#)
 - attributes, [264](#)
- Replace, [257](#), [267](#), [271](#), [272](#), [278](#)
- Replacement Part Number, [190](#)
- Reset ServerNet Statistics, [258](#)
- Reset Statistics, [263](#)
- Responsive Test, [146](#)
- Restore CLIM Configuration action, [99](#)

S

- SAC
 - about, [194](#)
 - actions, [196](#)
 - attributes, [195](#)
- sanitize disk, [226](#)
- SAS Card
 - about, [196](#)
- SAS Disk, [116](#)
- SCSI Controller
 - about, [199](#)
 - actions, [200](#)
 - attributes, [199](#)
- SCSI Extender, [211](#)
- SCSI SAC see SSAC
- SCSI-to-Fiber Converter, [211](#)
- select CLIMs to be registered,
- server certificate,
- ServerNet
 - cluster, [262](#)
 - cluster actions, [263](#)
 - cluster attributes, [262](#)
 - external fabric, [259](#)
 - internal fabric, [155](#), [156](#)
 - Local Node, [264](#)
 - Local Node actions, [264](#)
 - Local Node attributes, [264](#)
 - Remote Node, [264](#)
 - Remote Node actions, [265](#)
 - Remote Node attributes , [264](#)
- ServerNet II Switch
 - about, [265](#)
 - actions, [266](#)
 - attributes, [266](#)
- ServerNet Path Test on X Fabric, [258](#)
- ServerNet Path Test on Y Fabric, [259](#)
- ServerNet PIC

- about, [200](#), [201](#)
- actions, [202](#)
- attributes, [201](#)
- ServerNet Port, [202](#)
- attributes, [203](#)
- ServerNet Switch
 - about, [203](#)
 - attributes, [203](#)
- ServerNet Switch Board
 - about, [205](#)
 - actions, [206](#)
 - attributes, [205](#)
- ServerNet/DA see about
- Service Processor (SP)
 - about, [207](#)
 - actions, [209](#)
 - attributes, [207](#)
- Service State values, [246](#)
- Set Data Collection Volume, [227](#)
- Set Days to Persist for Diagnostic Data, [227](#)
- Set Fabric Setting, [267](#)
- Set Location for CLIM Log Collection, [102](#)
- Set ServerNet Cluster State, [259](#), [263](#)
- Set System Type, [227](#)
- Show CLIM/Key Manager Registration Information, [99](#)
- Smart Array Controller, [209](#)
- SNDA
 - about, [210](#)
 - actions, [210](#)
 - attributes, [210](#)
- Soft Reset, [267](#), [271](#)
- SSAC
 - about, [211](#)
 - actions, [211](#)
 - attributes, [211](#)
- Storage Router
 - about, [211](#)
 - actions, [213](#)
 - attributes, [212](#)
- Suppress Problem Incident Report Creation, [227](#)
- SWAN Battery
 - about, [215](#)
 - attributes, [216](#)
- SWAN CLIP
 - about, [216](#)
 - actions, [217](#)
 - attributes, [216](#)
- SWAN Collection
 - about, [218](#)
- SWAN Fan
 - about, [218](#)
 - actions, [218](#)
 - attributes, [218](#)
- SWAN LAN Logic Board see about
- SWAN LANLB
 - about, [218](#)
 - actions, [219](#)
 - attributes, [219](#)
- SWAN Line

- about, [219](#)
- actions, [220](#)
- attributes, [219](#)
- SWAN Path
 - about, [220](#)
 - actions, [220](#)
 - attributes, [220](#)
- SWAN Power Supply see SWAN PS
- SWAN PS
 - about, [221](#)
 - actions, [221](#)
 - attributes, [221](#)
- SWAN/SWAN2 CRU
 - about, [213](#)
 - actions, [215](#)
 - attributes, [214](#)
- Switch Fan
 - about, [267](#)
 - actions, [268](#)
 - attributes, [268](#)
- Switch Group
 - about, [268](#)
- Switch Logic Board
 - about, [269](#)
 - actions, [270](#)
 - attributes, [269](#)
- Switch Node Port
 - about, [274](#)
 - actions, [275](#)
 - attributes, [274](#)
- Switch PIC
 - about, [271](#)
 - actions, [272](#)
 - attributes, [271](#)
- Switch Port
 - about, [276](#)
 - attributes, [276](#)
- Switch Power Supply
 - about, [272](#)
 - actions, [273](#)
 - attributes, [272](#)
- Switch SANMAN Process Pair, [263](#)
- Switch SNETMON Process Pair, [263](#)
- Switch-to-Node PIC
 - about, [273](#)
 - attributes, [273](#)
- Switch-to-Switch PIC
 - about, [275](#)
 - attributes, [275](#)
- Synchronize iLO Clocks to NonStop Clock, [227](#)
- System
 - about, [221](#)
 - actions, [223](#)
 - attributes, [221](#)
- system
 - locating resources, [76](#)
 - managing, [76](#)
 - monitoring resources, [76](#)
 - performing actions, [76](#)

- viewing resources, [76](#)
- system hang, recovery, [228](#)
- System Power Off, [227](#)
- system resources
 - list of, [77](#)
- System Serial Number, [222](#)
- System Type, [222](#)

T

- Tape
 - about, [229](#)
 - actions, [231](#)
 - attributes, [229](#)
- Tape Collection
 - about, [228](#)
- TCP/IP stack,
- Test Incident Report Delivery Paths, [227](#)
- tiers, defining,
- Token Ring ServerNet Adapter CRU see TRSA CRU
- TRSA CRU
 - about, [232](#)
 - actions, [232](#)
 - attributes, [232](#)
- trusted Local CA,

U

- unknown CRU
 - about, [233](#)
 - actions, [233](#)
- Unsuppress Problem Incident Report Creation, [228](#)
- Update Firmware, [267](#)
- Update Running Core License, [228](#)
- Update Topology, [263](#)
- UPS (6770 Switch Module)
 - about, [277](#)
 - actions, [278](#)
 - attributes, [277](#)
- UPS (IOAM)
 - about, [233](#)
 - actions, [234](#)
 - attributes, [233](#)

V

- V4SE, V8SE, [152](#), [239](#)
- Verify Power Fail Configuration, [228](#)
- Versatile Ethernet ServerNet enclosure, [152](#), [239](#)
- VIO
 - attributes, [240](#)
- VIO enclosure
 - (represented in OSM by VIO Module object), [239](#)
- VIO Fan
 - actions, [133](#)
 - attributes, [133](#)
- VIO FCSA
 - about, [234](#)
- VIO G4SA
 - about, [236](#)
 - actions, [237](#)
 - attributes, [236](#)

VIO Logic Board

about, [237](#)

actions, [238](#)

attributes, [237](#)

VIO Module

about, [239](#)

actions, [241](#)

VIO Power Supply

actions, [186](#)

W

window

printing, [51](#)

X

X Fabric Responsive Test, [261](#)

X Fabric ServerNet State , [163](#)

X.509 certificate, use existing Client Certificate,

Y

Y Fabric Responsive Test, [261](#)

Y Fabric ServerNet State , [163](#)

15 Register CLIMs with Key Managers Guided Procedure Online Help

Introduction

The Register CLIMs with Key Managers Guided Procedure guides you through the process of registering storage CLIMs with a cluster of HP Enterprise Secure Key Managers (ESKMs) for the purpose of providing encryption on storage devices. Keys generated by the Key Managers help protect your storage data.

NOTE: See the *NonStop Volume Level Encryption Guide* for steps that must be taken before performing this guided procedure. The manual also provides information on the NonStop encryption product, including encryption principles, techniques, system requirements and planning information.

The online help topics are accessed through Help buttons on the major windows and dialog boxes within the procedure. The topics, organized to match the steps in the guided procedure, include:

- [Selecting CLIMs to Be Registered](#)
- [Configuring a Key Manager Cluster](#)
- [Creating CLIM Group, Username, and Password](#)
- [Using the Select the Local CA Dialog Box](#)
- [Selecting Certification Method and Creating Client Certificates](#)
- [Creating Client Certificate Automatically](#)
- [Use Your Own X.509 Certificate](#)
- [Registering CLIMs](#)

Selecting CLIMs to Be Registered

Upon [starting](#) the guided procedure, it displays the Storage CLIM Selection dialog box, from which you select the CLIMs to be registered with a Key Manager Cluster. Only storage CLIMs with model G5 and later are listed in the dialog box.

OSM8 - Storage CLIM Selection

Select and add storage CLIMs to be registered with Key Managers.

Logical					
	Resource Name	X1 Fabric Connection State	Y1 Fabric Connection State	Configured Operation Mode	Storage Software
	CLIM \$ZZCIP.C100231	Correctly Connected	Correctly Connected	Storage	T0830H01_21AUG
	CLIM \$ZZCIP.C100232	Correctly Connected	Correctly Connected	Storage	T0830H01_21AUG
	CLIM \$ZZCIP.C100233	Not Connected	Not Connected	Storage	

Logical					
	Resource Name	X1 Fabric Connection State	Y1 Fabric Connection State	Configured Operation Mode	Storage S
<input type="radio"/>	CLIM \$ZZCIP.C100231	Correctly Connected	Correctly Connected	Storage	T0830H01_
<input type="radio"/>	CLIM \$ZZCIP.C100232	Correctly Connected	Correctly Connected	Storage	T0830H01_

All CLIMs to be registered must be selected and moved from the upper to the lower list using the **Add** or **Add All** buttons (the Ctrl key can be used to select multiple CLIMs). **Remove** or **Remove All** can be used to remove CLIMs from the list to be registered.

Once all CLIMs to be registered have been moved to the lower list, click **Continue** to proceed to the next step of the guided procedure: [Configuring a Key Manager Cluster](#).

Configuring a Key Manager Cluster

NOTE: The Key Manager Cluster must be created by an administrator through the Key Manager interface. For more information, see the *NonStop Volume Level Encryption Guide*. This step of the guided procedure allows you to configure the existing cluster by organizing the Key Managers into tiers. Although all Key Managers in a cluster are peers and share all keys and clients, the clients can be configured to view the cluster in tiers and prefer nearby Key Manager Cluster members for key services. This is advantageous for optimizing request latency and network traffic.

Upon [selecting the CLIMs](#) in the Storage CLIM Selection dialog box and clicking **Continue**, the Encryption Key Manager Cluster Configuration Information dialog box is displayed. In this dialog box, you will:

- [Define Key Manager Tiers for CLIMs](#)
- [Enter Credentials and TCP/IP Stack](#)
- [Check Connectivity to Key Managers](#)

Defining Key Manager Tiers for CLIMs

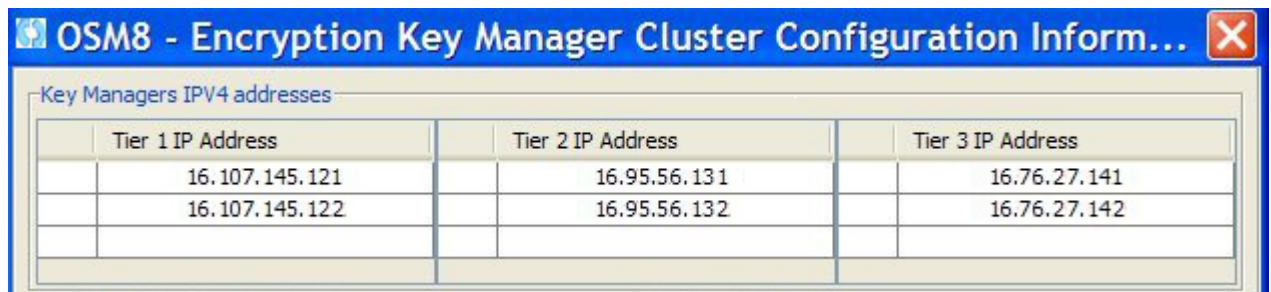
This step of the guided procedure allows you to configure the CLIMs view of an existing cluster by organizing the Key Managers into multiple levels of load-balancing groups. A load-balancing group is a group of Key Managers the CLIMs can connect to. The multi-tier feature provides for additional failover support by allowing CLIMs to failover to the next tier if the higher tier becomes unavailable. Cluster nodes that are located in the same geographical location are recommended to be added to the same tier, with the first tier containing local or nearby Key Managers.

You can define up to three tiers by providing the IPv4 addresses for Key Managers that are all members of the same Key Manager Cluster. At least two Key Managers should be specified in Tier 1. You are not required to enter Key Managers in Tier 2 or 3; however, you cannot skip over a tier. In order to enter Key Managers in Tier 3, you must also enter at least one in Tier 2. There is no maximum limit to the number of Key Managers defined in a tier. Do not list a Key Manager more than once in the tier configuration.

Examples:

- One usage scenario or “best practice” example is to use Tier 1 for local Key Managers, Tier 2 for remote Key Managers, and Tier 3 for the Key Managers at a disaster recovery site.
- The example pictured below shows a recommended configuration of at least two Key Managers in each tier. If you have just four Key Managers in the cluster, placing two local Key Managers in Tier 1 and two remote Key Managers in Tier 2 would be recommended.

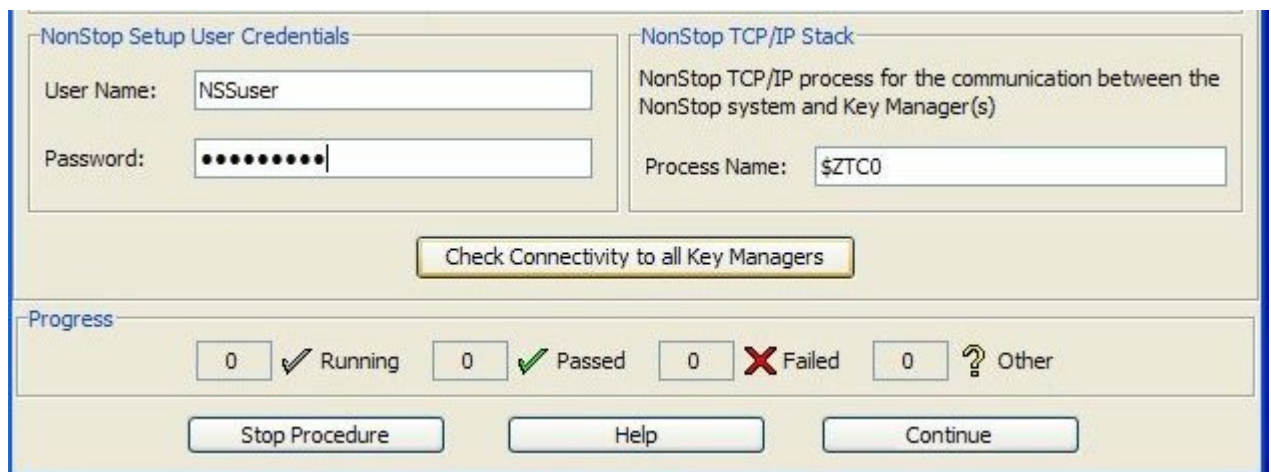
When you have finished defining the tier configuration, proceed to [enter the NonStop Setup User Credentials and TCP/IP Stack](#).



Tier 1 IP Address	Tier 2 IP Address	Tier 3 IP Address
16.107.145.121	16.95.56.131	16.76.27.141
16.107.145.122	16.95.56.132	16.76.27.142

Entering Credentials and TCP/IP Stack

After you have [defined the Key Manager tiers](#), you must provide a valid user name and password for the NonStop Setup User (NSSuser) Credentials and specify the NonStop TCP/IP stack in the middle panel of the Encryption Key Manager Cluster Configuration Information dialog box (pictured below). The user name and password must be configured beforehand, by an administrator in the Key Manager interface. A valid NonStop Setup User will have permission to create the user name and password for each CLIM client on the Key Manager. The NonStop TCP/IP stack is the stack that the guided procedure will use to communicate with the Key Managers.



NonStop Setup User Credentials

User Name:

Password:

NonStop TCP/IP Stack

NonStop TCP/IP process for the communication between the NonStop system and Key Manager(s)

Process Name:

Progress

0 ☒ Running 0 ☒ Passed 0 ☒ Failed 0 ☒ Other

Once the credentials and TCP/IP stack have been entered, the [Check Connectivity of Key Managers](#) button becomes active. You must click that button to proceed; the **Continue** button remains inactive until the status for all Key Manager connectivity is obtained and reported.

Checking Connectivity to Key Managers

Upon clicking the **Check connectivity to all Key Managers** button, the guided procedure checks the connectivity by attempting to log on to each Key Manager. The connectivity status for each Key Manager is reported in the column to the left of its IP address with a green check mark (for success) or a red "X" (for failure). Also, as each connection attempt is made, a running count of the passes and failures is reported in the Progress section of the dialog box.

Key Managers IPv4 addresses					
	Tier 1 IP Address		Tier 2 IP Address		Tier 3 IP Address
✓	16.107.145.121	✓	16.95.56.131	✓	16.76.27.141
✓	16.107.145.122	✓	16.95.56.132	✓	16.76.27.142

NonStop Setup User Credentials

User Name:

Password:

NonStop TCP/IP Stack

NonStop TCP/IP process for the communication between the NonStop system and Key Manager(s)

Process Name:

Progress

0 ☐ Running 6 ☒ Passed 0 ☒ Failed 0 ☐ ? Other

The **Continue** button remains inactive until all Key Managers have been checked for connectivity and at least one Key Manager has been successfully connected to. If no Key Managers pass the connectivity check, an error message is displayed.

⚠ WARNING! You should troubleshoot Key Managers with failed connections and, upon correcting the problem, click **Check connectivity to all Key Managers** again. You can continue the procedure using the Key Managers that did pass the check; however, the registered CLIMs would not be able to take advantage of the additional load-balancing or failover provided by the Key Managers that failed the connectivity check. In particular, continuing the procedure if only one Key Manager passes the connectivity test is not advised; that lone Key Manager would constitute a potential single point of failure for the NonStop system.

Removing a nonresponsive Key Manager from a cluster is done only by an administrator through the Key Manager interface, although that action is not required for the purposes of this procedure. When you are satisfied with the configuration information, click **Continue** to go proceed to the next step of the guided procedure: [Creating CLIM Group, Username, and Password](#)

Creating CLIM Group, Username, and Password

Upon clicking **Continue** in the [Encryption Key Manager Cluster Configuration Information dialog box](#), the Create CLIM Client Username and Password dialog box is displayed. This step of the procedure creates a CLIM group, username, and password on the Key Manager for all selected CLIMs.

OSM8 - Create CLIM Client Username and Password

CLIM Client Group Name:

Click to create user ID and password for each CLIM Client.

CLIMs

	Resource Name	Status
✓	CLIM \$ZZCIP.C100231	User ID/Password created successfully
✓	CLIM \$ZZCIP.C100232	User ID/Password created successfully

Progress

0 ☒ Running 1 ☒ Passed 0 ☒ Failed 0 ☒ Other

In the top portion of the dialog box, the CLIM Client Group Name box displays the name ("NonStop") of the CLIM group created by the guided procedure (if not already created).

Click **Create User IDs/Passwords**. The guided procedure then:

- Verifies NSSuser logon information by attempting to logon to a Key Manager. If a logon failure occurs on the first Key Manager, the next Key Manager is attempted (and so on). If no Key Manager can be logged onto, an error message is displayed.
- Creates a username and password on the Key Manager for each listed CLIM and, if the CLIM group does not exist, it will be created also. The usernames will be in the form: **S<system number>< CLIM name>**. For example: **S00262C100233** represents a system number of **00262** and CLIM name of **C100233**.
- Reports the status of the operation for each individual CLIM, along with a running count of the passes and failures in the Progress section of the dialog box.

NOTE: In addition to the status reported in the Progress section of this dialog box, status and error messages are also reported in the "Messages" panel of the guided procedure main window and saved to a log file.

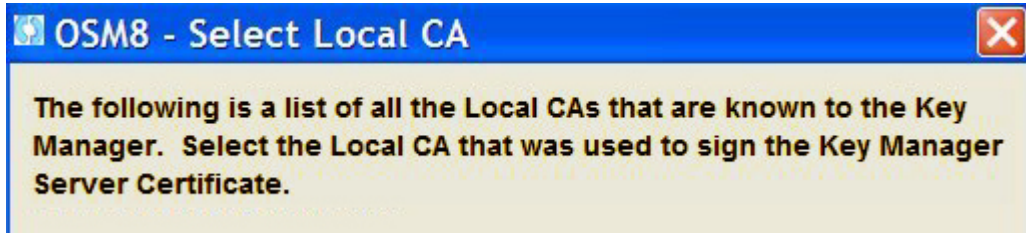
Once the action completes and is successful on at least one CLIM, the **Continue** button becomes active. Click **Continue** to go to the next step in the procedure: [Selecting the Local CA that Signed the Server Certificate](#).

NOTE: Upon clicking **Continue**, any CLIMs that failed this step of the procedure are removed from the list of CLIMs to be registered; a pop-up dialog box lists any CLIMs that were removed.

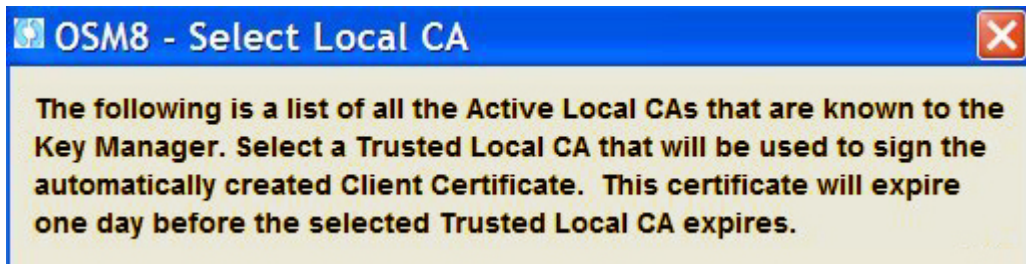
Using the Select the Local CA Dialog Box

NOTE: The Select Local CA dialog box is displayed twice during the guided procedure *if* you choose to have your Client Certificates automatically created. To view the appropriate help topic when clicking the Help button on that dialog box:

- If the text at the top of the dialog box is as pictured below, see [Selecting the Local CA that Signed the Server Certificate](#).



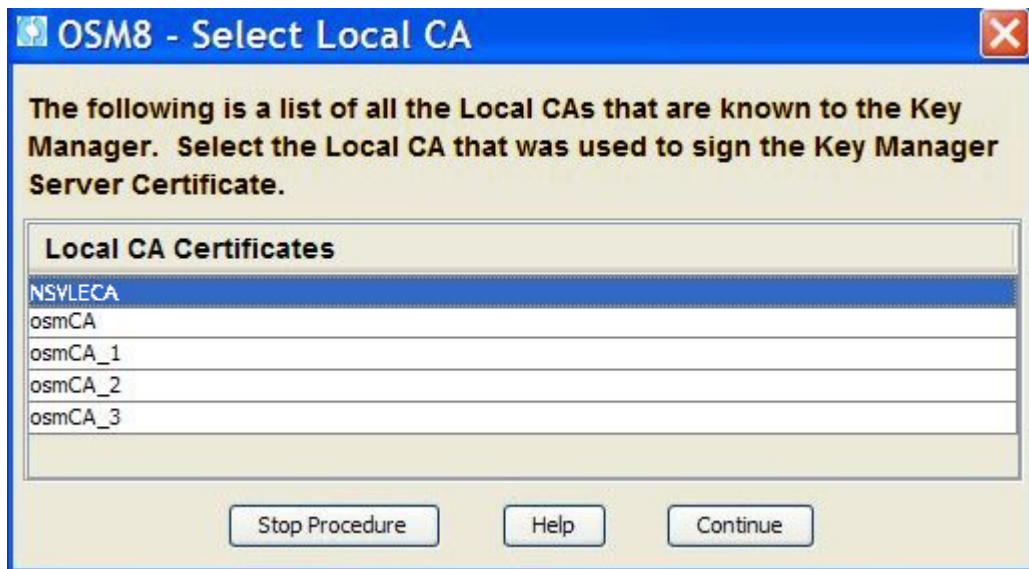
- If the text at the top of the dialog box is as pictured below, see [Creating Client Certificate Automatically](#) for the appropriate help topic.



Selecting the Local CA that Signed the Server Certificate

After successfully [creating the CLIM group, username, and password](#), the next step is to select the Local CA that was used to sign the Key Manager Server certificate for SSL (Secure Sockets Layer).

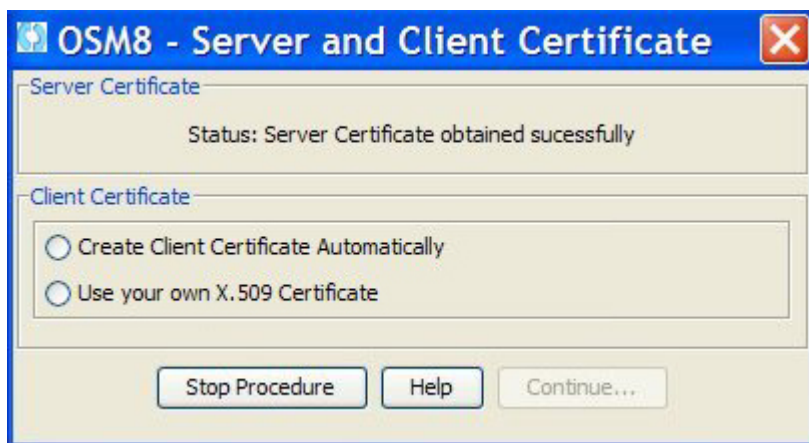
The Select Local CA dialog box displays a list of all Local CAs stored on the Key Manager cluster. From this list, you must select the Local CA that was used to sign the Key Manager Server certificate for SSL. Once selected, the **Continue** button becomes active. If no Local CAs are available or an error occurred while obtaining the list, an error message is displayed and the **Continue** button remains inactive.



Click Continue to proceed to the next step of the guided procedure: [Selecting Certification Method and Creating Client Certificates](#).

Selecting Certification Method and Creating Client Certificates

Upon [selecting the Local CA that signed the Server Certificate](#), the Server and Client Certificate dialog box is displayed. This dialog box reports the status of OSM's attempt to obtain information from the Local CA specified in the previous step and prompts you to decide what certificate(s) the guided procedure will use to register CLIMs.



The guided procedure automatically obtains information about the Local CA that signed the server certificate and reports the status of that operation in the top portion of the dialog box under the "Server Certificate" heading as either:

- Server Certificate obtained successfully
- Error!! Unable to obtain the Local CA that signed the server certificate

While the Local CA information is being obtained, the lower portion of the dialog box is inactive. If an error occurs during this process, an error message is displayed in a pop-up dialog box, and also in the "Messages" panel of the guided procedure main window.

Create or Use Existing Client Certificate

Once the Local CA information has been obtained successfully, you must choose between:

- [Creating Client Certificate Automatically](#) – having the guided procedure create a client certificate for each CLIM automatically.
- [Using your own X.509 Certificate](#) – whereby you supply information so that OSM can use an existing signed X.509 Certificate to each register CLIM.

After making your selection, click **Continue** to proceed to the step of the procedure, depending on the option chosen.

Creating Client Certificate Automatically

Having [chosen](#) to create client certificates automatically, the Select Local CA dialog box is displayed once again, this time showing a list of the Local CAs stored on the Key Manager cluster that are in the Active state. From this list, select a trusted Local CA to be used to sign the client certificates for each CLIM.

NOTE: The “Active” CAs displayed in this dialog box are the Local CAs known to the Key Managers that will not expire for at least 31 days. To make sure you are selecting a Local CA that is both “trusted” and has an expiration date suitable for the certificates you will create, log on to a Key Manager interface and select the **Security** tab:

- To check expiration dates of the available Local CAs, click the **Local CAs** link located under the “Certificates & CAs” heading in the left column of the page. Note that the client certificates you create automatically through the OSM guided procedure will expire one day before the expiration date of the Local CA used to sign them.
- After identifying a Local CA with a suitable expiration date, click the **Trusted CA Lists** link, also located under the “Certificates & CAs” heading in the left column on the Security tab. On that page, click **Properties**. If your Local CA of choice is not listed among the Trusted CAs, click **Edit** and use the **Add** button to move the Local CA to the “Trusted CAs” list.



After selecting the desired Local CA in the Select Local CA dialog box, click **Continue**. The guided procedure then displays the Create Client Certificate Automatically dialog box. It is populated with the list of CLIMs to be registered (the list originally selected, minus any that failed any prior step in the guided procedure). Select a certificate key size of either 1024 bit or 2048 bit, then click the **Create CLIM Client Certificates** button to start the process of creating the client certificates.

NOTE: The default certificate key size is 1024 bit, but 2048 bit is required by ESKM 3.0.

OSM8 - Create Client Certificate Automatically

Select Key Size and click to automatically create a unique Client Certificate for each CLIM.

Certificate Key Size

☐ 1024 bit ☒ 2048 bit

Create CLIM Client Certificates

CLIMs

	Resource Name	Status
✓	CLIM \$ZZCIP.C100233	Client Certificate created successfully
✓	CLIM \$ZZCIP.C100231	Client Certificate created successfully

Progress

0 ✓ Running 2 ✓ Passed 0 ✗ Failed 0 ? Other

Stop Procedure Help Continue

Upon clicking **Create CLIM Client Certificates**, the guided procedure starts the process of creating the client certificates, including a private key and a cryptographically secure pass phrase for each of the CLIMs listed in the table. The selected Local CA will be used to validate the client certificate during the SSL handshake.

As with other guided procedure operations, the status is reported for each CLIM and by a running total in the Progress section of the dialog box. Details of any error can be seen by clicking on the row of the CLIM reporting the error.

After the process has completed (either passing or failing on all of the CLIMs listed), click **Continue** to proceed to the final step of the guided procedure: [Register CLIMs](#). CLIMs for which the client certificate creation process failed will be removed from the list of CLIMs to be registered; a pop-up dialog informs you of any such removals.

Use Your Own X.509 Certificate

Having [chosen](#) to have OSM use your own signed X.509 Certificate, the "Use your own X.509 Certificate" dialog box is displayed. In this dialog box, you must copy and paste information from your own signed X.509 Certificate for each CLIM to be registered.

The following rules apply to the certificate(s) you are copying from (each CLIM requires a separate certificate):

- When the certificate is created, it must contain the username of the CLIM in the Common Name (CN) field, in the form **S<system number>< CLIM name>** (as created during the [create CLIM group, username, and password](#) step).
- It must be a signed certificate.
- If it was signed by a CA not known to one of the Key Managers you are using (in other words, not a Local CA), it must be imported into one of those Key Managers before completing this guided procedure. For information on how to import a CA into a Key Manager, see the *Enterprise Secure Key Manager Users Guide*.

- The certificate must be added to the Default Trusted CA List in one of the Key Managers. For information on how to do this, see the *NonStop Volume Level Encryption Guide*.
- OSM can only validate up to 128 bit certificates. If you copy and paste from certificates with higher bit counts, those certificates will neither pass nor fail the **Check Certificate Validity** step – the guided procedure displays a “?” (question mark) rather than a red “X” or a green check mark – but allows you to continue with the procedure and use those certificates to register a CLIMs.

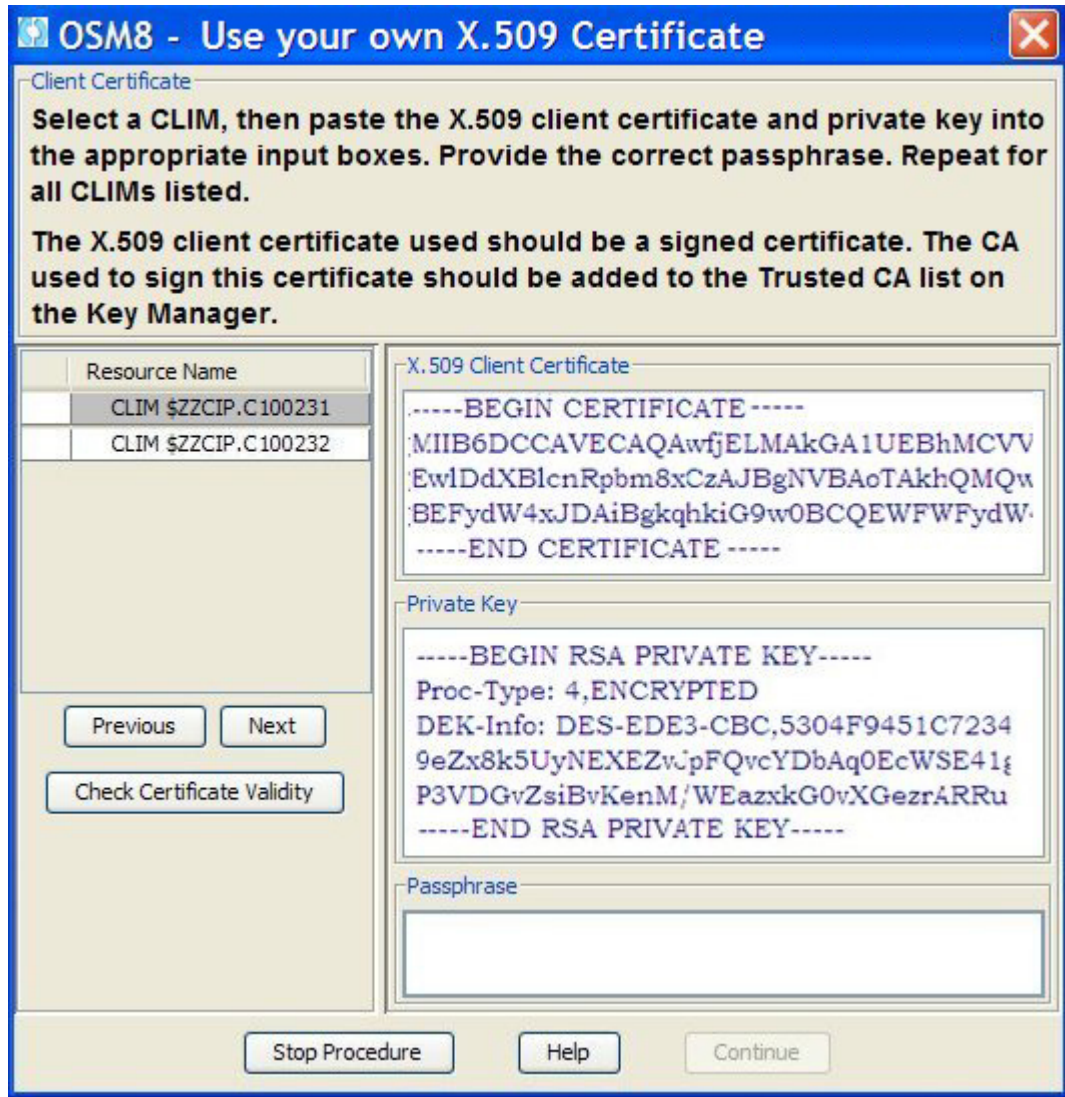
NOTE: In such cases, OSM also displays a message instructing how you can (optionally) download a java library required in order for OSM to validate those certificates. This process requires you to restart the OSM Service Connection and the guided procedure. It is necessary only if you wish to have OSM validate those certificates with a bit count higher than 128; it is not required to continue with the guided procedure and use those unvalidated certificates to register CLIMs.

To provide OSM with the certificate information for each CLIM listed, locate and open your signed X.509 certificate, then in this guided procedure dialog box, perform the following steps:

1. From the list of CLIMs in the left box, click to select a CLIM.
2. Copying from your own signed X.509 certificate, paste (or type) the appropriate information into the boxes titled:
 - X.509 client certificate
 - Private Key
 - Passphrase (the input for this field will be echoed back as "*****")
3. Select another CLIM, by clicking on it or by using the **Next** or **Previous** buttons, and repeat step 2 for that CLIM's client certificate. A circle is displayed in the left column for CLIMs in which the required three fields have been completed. Continue the process until the information is provided for each CLIM in the list.
4. Once the fields have been completed for all CLIMs, the **Check Certificate Validity** button becomes active. Upon clicking it, the guided procedure checks to make sure that the combination of certificate, key, and passphrase are correct for each of the CLIMs. If the verification passes, a green check mark is placed next to the CLIM name (replacing the circle icon). If the verification fails, a red "X" is placed next to the CLIM name. If OSM is unable to verify (as in the case of certificates with a bit count over 128, for example) a "?" (question mark) is placed next to the CLIM name. The **Continue** button becomes active only after the validity check for all CLIM client certificates has completed. If errors are reported, you can go back and click on the CLIM reporting the error and alter the appropriate input box (errors are

indicated by red italic text). You can correct the error and repeat the validity check, or go on to step 5 to complete the registration process for the CLIMs that did not fail the validity check.

5. Click **Continue** to proceed to the final step of the guided procedure: [Register CLIMs](#). CLIMs for which the validity check failed will be removed from the list of CLIMs to be registered; a pop-up dialog informs you of any such removals.



The dialog box is titled "OSM8 - Use your own X.509 Certificate". It contains instructions for selecting a CLIM and pasting an X.509 client certificate and private key. It includes a table for selecting a CLIM, input fields for the certificate and private key, a passphrase field, and buttons for "Previous", "Next", "Check Certificate Validity", "Stop Procedure", "Help", and "Continue".

Client Certificate

Select a CLIM, then paste the X.509 client certificate and private key into the appropriate input boxes. Provide the correct passphrase. Repeat for all CLIMs listed.

The X.509 client certificate used should be a signed certificate. The CA used to sign this certificate should be added to the Trusted CA list on the Key Manager.

Resource Name
CLIM \$ZZCIP.C100231
CLIM \$ZZCIP.C100232

Previous Next

Check Certificate Validity

X.509 Client Certificate

```
-----BEGIN CERTIFICATE-----
MIIB6DCCAWECAQAwfjELMAkGA1UEBhMCVV
EwIDdXB1cnRpbm8xCzAJBgNVBAsTAKhQMqW
BEFydW4xJDAiBgkqhkiG9w0BCQEFWFydW
-----END CERTIFICATE-----
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5304F9451C7234
9eZx8k5UyNEXEZvJpFQvcYDbAq0EcWSE41g
P3VDGvZsiBvKenM/WEazxkG0vXGezrARRu
-----END RSA PRIVATE KEY-----
```

Passphrase

Stop Procedure Help Continue

Registering CLIMs

The final step of the guided procedure is to register the CLIMs with the Key Manager Cluster. Upon successful [creation or input of client certificates](#), the Key Manager/CLIM Registration dialog box is displayed. This dialog box shows a list of all the CLIMs that were selected for registration to the Key Manager Cluster, minus any that may have been removed because of errors encountered during prior steps of this procedure.

Click the **Register CLIMs to Key Manager Cluster** button to begin the registration process.



After each registration attempt, the success or failure for each CLIM is reported in the far left column (a green check mark indicates success, a red "X" indicates failure). The Progress section toward the bottom of the dialog box displays a running count of the passes and failures. Details for any error are available by clicking on the row of the CLIM reporting the error.

Reminder to Delete the NSSuser user from the Key Manager

Once the registration process has completed and you click Continue in Key Manager/CLIM Registration dialog box, a final dialog box reminds you that the NSSuser user must be manually deleted by an administrator in the Key Manager interface.



The final message displayed in the "Messages" panel of the guided procedure main window should be either: "Procedure completed successfully," "Procedure terminated by user," or "Procedure terminated due to error." A log file compiles all of the messages that were displayed in the "Messages" panel during the various steps of the guided procedure.